NUCLEAR SECURITY: CAN DOE MEET PHYSICAL FACILITY SECURITY REQUIREMENT

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

APRIL 27, 2004

Serial No. 108–207

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

96–313 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

CONTENTS

NUCLEAR SECURITY: CAN DOE MEET PHYSICAL FACILITY SECURITY REQUIREMENT

TUESDAY, APRIL 27, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:04 a.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays and Watson.

Staff present: Lawrence Halloran, staff director and counsel; J. Vincent Chase, chief investigator; Thomas Costa, professional staff member; Robert Briggs, clerk; Jean Gosa, minority assistant clerk; and Andrew Su, minority professional staff member.

Mr. SHAYS. I call this hearing of the Subcommittee on National Security, Emerging Threats and International Relations to order.

Today, we continue our oversight of physical security at the Nation's nuclear weapons facilities. Last June, we learned the Department of Energy [DOE], was not aggressively confronting the many challenges posed by the need to secure a sprawling, aging infrastructure against post-September 11th threats.

So we asked the GAO to evaluate the development and implementation of the new security standard called the design basis threat [DBT].

The GAO report released today finds some progress, but concludes the new DBT may not be as realistic, rigorous, or real-time as needed to protect nuclear materials from determined terrorists.

Without question, DOE nuclear warhead production plants, testing facilities, research labs, storage locations, and decommissioned sites are attractive targets for terrorists determined to turn our technology against us and willing to die while doing so. The highly enriched uranium and plutonium held at various locations could be used as the core of an improvised nuclear device or dispersed as a radiological weapon.

Yet, it took almost 2 years and an inexplicably and inexcusably long time to update the DBT after September 11th.

Faced with a new security imperative to deny access, not just contain or catch intruders, it should have been immediately obvious DOE has too many facilities housing nuclear materials. And those facilities are old, above ground, scattered around cluttered World War II era plant configurations and not buffered by adequate setback space.

It may not be enough just to harden existing sites with more gates, guns, and guards. Consolidation of nuclear material storage, long advocated, but little pursued at DOE, would improve security by reducing the number of sites and the cost of protecting them.

New security technologies will have to be evaluated and deployed to meet emerging threats. But as we will hear in testimony today, a serious question remains whether the DBT adequately reflects the true nature of the threat. Some believe the design basis threat might be more accurately called the dollar-based threat, reflecting only a watered down measure of how much security the Department can afford. Additionally, GAO doubts DOE will be able to fully implement even that standard before 2009. We know that terrorists will not wait that long to try to exploit lingering vulnerabilities in our nuclear complex defenses.

Last month, DOE announced a plan to move some nuclear material from Technical Area 18 at the Los Alamos National Laboratory to a more secure facility in Nevada. Implementation of that plan will demonstrate a sharper focus and renewed sense of urgency at DOE and the National Nuclear Security Administration [NNSA], but we need to be sure that consolidation is just the most visible part of a broad strategic effort to implement a realistic DBT.

Charged by law to sustain the Nation's nuclear deterrent capabilities, DOE and NNSA have the unenviable task of balancing the demands of that mission against the risks and costs of meeting security threats in a new and dangerous era. Our oversight seeks to ensure that balance is struck as openly and as effectively as possible so that nuclear security, Homeland Security, and national security will be enhanced. Those are goals shared by all our witnesses, and we are grateful for their participation in this hearing. We welcome them, and we look forward to their testimony.

[NOTE.—The GAO report entitled, "Nuclear Security, DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat," may be found in subcommittee files.]

[The prepared statement of Hon. Christopher Shays follows:]

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382

Statement of Rep. Christopher Shays
April 27, 2004

Today we continue our oversight of physical security at the nation's nuclear weapons facilities. Last June, we learned the Department of Energy (DoE) was not aggressively confronting the many challenges posed by the need to secure a sprawling, aging infrastructure against post-September 11th threats. So we asked the General Accounting Office (GAO) to evaluate the development and implementation of the new nuclear security standard – called the "Design Basis Threat" or DBT.

The GAO report, released today, finds some progress but concludes the new DBT may not yet be as realistic, rigorous or real-time as needed to protect nuclear materials from determined terrorists. Without question, DoE nuclear warhead production plants, test facilities, research labs, storage locations and decommissioned sites are attractive targets for terrorists determined to turn our technology against us, and willing to die while doing so. The highly enriched uranium and plutonium held at various locations could be used as the core of an improvised nuclear device or dispersed as a radiological weapon.

Yet it took almost two years - an inexplicably and inexcusably long time - to update the DBT after September 11th.

Faced with the new security imperative to deny access, not just contain or catch intruders, it should have been immediately obvious DOE has too many facilities housing nuclear materials. And those facilities are old, above ground, scattered around cluttered World War II era plant configurations and not buffered by adequate setback space.

It may not be enough just to harden existing sites with more gates, guns and guards. Consolidation of nuclear material storage, long advocated but little pursued at DoE, would improve security by reducing the number of sites and the cost of protecting them. New security technologies will have to be evaluated and deployed to meet emerging threats.

But as we will hear in testimony today, a serious question remains whether the DBT adequately reflects the true nature of the threat. Some believe the Design Basis Threat might be more accurately called the "Dollar Based Threat" reflecting only a watered down measure of how much security the Department can afford. And, GAO doubts DOE will be able to fully implement even that standard before 2009. We know the terrorists will not wait that long to try to exploit lingering vulnerabilities in our nuclear complex defenses.

Last month, DOE announced a plan to move some nuclear material from Technical Area 18 at the Los Alamos National Laboratory to a more secure facility in Nevada. Implementation of that plan will demonstrate a sharper focus and renewed sense of urgency at DOE and the National Nuclear Security Administration (NNSA). But we need to be sure that consolidation is just the most visible part of a broad, strategic effort to implement a realistic DBT.

Charged by law to sustain the nation's nuclear deterrent capabilities, DOE and NNSA have the unenviable task of balancing the demands of that mission against the risks and costs of meeting security threats in a new and dangerous era. Our oversight seeks to ensure that balance is struck as openly and as effectively as possible so that nuclear security, homeland security and national security will be enhanced.

Those are goals shared by all our witnesses, and we are grateful for their participation in this hearing. Welcome. We look forward to your testimony.

Mr. SHAYS. At this time, I will recognize and then swear in Robin M. Nazzaro, Director, National Resources and Environment, U.S. General Accounting Office, accompanied by James Noel, Assistant Director, National Resources and Environment, U.S. General Accounting Office. And Danielle Brian, executive director, Project On Government Oversight. At this time, if you would stand.

Is there anyone else that possibly would be responding? If so, I would like for them to stand to be sworn in just in case.

[Witnesses sworn.]

Mr. SHAYS. Note for the record our witnesses have responded in the affirmative.

We will basically have a statement by Director Nazzaro, and then we will invite Mr. Noel and Ms. Brian to respond to questions as well.

Excuse me. We do have testimony? I'm sorry, I apologize.

So Mr. Noel, you are the only one who does not have testimony but will respond to questions. Is that correct?

Mr. NOEL. Correct.

Mr. SHAYS. OK. Thank you. I will get it together here.

Welcome.

STATEMENTS OF ROBIN M. NAZZARO, DIRECTOR, NATURAL RESOURCES AND ENVIRONMENT, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY JAMES NOEL, ASSISTANT DIRECTOR, NATIONAL RESOURCES AND ENVIRONMENT, U.S. GENERAL ACCOUNTING OFFICE; AND DANIELLE BRIAN, EXECUTIVE DIRECTOR, PROJECT ON GOVERNMENT OVERSIGHT

Ms. NAZZARO. Thank you, Mr. Chairman.

I am pleased to be here today to discuss our report that you are issuing entitled, "Nuclear Security: DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat."

A successful terrorist attack on a site containing nuclear weapons or the material used in nuclear weapons could have devastating consequences. Because of these risks, DOE needs an effective safeguards and security program. A key component of such a program is the design basis threat [DBT], which is a classified document that identifies the potential size and capabilities of terrorist forces and is based on the postulated threat and intelligence community assessment of potential terrorist threats to nuclear weapons facilities.

Following the September 11, 2001, terrorist attacks, you asked us to review physical security at DOE sites that have Category I special nuclear material. These material include specified quantities of plutonium and highly enriched uranium.

Last year, I testified before this subcommittee that while DOE took immediate steps to improve security in the aftermath of the September 11th terrorist attacks, DOE's effort to develop and issue a new DBT took almost 2 years.

Today, I would like to focus on the implementation of the new DBT that was issued in May 2003. Specifically, my testimony focuses on our analysis of the higher threat contained in the new DBT and the remaining issues that we feel need to be resolved in

order for DOE to fully defend against the threat contained in the DBT.

With respect to our analysis of the 2003 DBT, we have two areas of concern. First, while we found that the new DBT is substantially more demanding than the previous one, the threat contained in the 2003 DBT is less than the threat identified in the postulated threat. Or, in other words, DOE is preparing to defend against a significantly smaller group of terrorists. Only for its sites and operations that handle nuclear weapons is DOE currently preparing to defend against an attacking force that approximates the lower range of the threat identified in the postulated threat.

For its other Category I special nuclear material sites, which may have improvised nuclear device concerns that, if successfully exploited by terrorists, could result in a nuclear detonation, DOE is only preparing to defend against a terrorist force that is significantly smaller than was identified in the postulated threat.

Our second concern with the DBT is that the Department's criteria for determining the severity of radiological, chemical, or biological sabotage may be insufficient. For example, the criterion used for protection against radiological sabotage is based on acute radiation doses received by individuals. This may not fully capture or characterize the damage that a major radiological disposal might cause. For example, a worst-case analysis at one DOE site showed that while radiological dispersal would not pose immediate, acute health problems for the general public, the public could experience measurable increases in cancer mortality over a period of decades after such an event. Moreover, releases at the site could also have environmental consequences requiring hundreds of millions to billions of dollars to clean up and affect the habitat of people who live within 10 miles of the sight.

Now, let me highlight the issues that we feel need to be resolved in order for DOE to fully defend against the threat contained in the new DBT. To date, DOE has not developed any official estimates of the overall costs of DBT implementation. More importantly, current DBT implementation cost estimates do not include items such as closing unneeded facilities, transporting and consolidating materials, completing line-item construction projects and other important activities that are outside the responsibility of the Safeguards and Security Programs budget. Finally, complicating the issue is the fact that the Secretary has not yet designated as called for in the new DBT which, if any, of DOE sites have improvised nuclear concerns. If a site is designated to have such a concern, it may be required to shift to a more demanding and costly protection strategy.

Bottom line, DOE is unlikely to meet its own fiscal year 2006 deadline for full implementation of the new DBT. Some sites estimate that it could take as long as 5 years given adequate funding.

In our report, we made seven recommendations to the Secretary of Energy that are intended to strengthen DOE's ability to meet the requirements of the new DBT, improve the Department's ability to deal with future terrorist threats, and to better inform Congress on departmental progress in meeting the threat contained in the DBT and reducing risks to critical facilities at DOE sites.

Mr. Chairman, that concludes my statement. I would be happy to respond to any questions you may have.

[The prepared statement of Ms. Nazzaro follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, April 27, 2004

NUCLEAR SECURITY

DOE Must Address Significant Issues to Meet the Requirements of the New Design Basis Threat

Statement of Robin M. Nazzaro, Director
Natural Resources and Environment Team

GAO-04-701T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-04-701T, a testimony to the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

A successful terrorist attack on Department of Energy (DOE) sites containing nuclear weapons or the material used in nuclear weapons could have devastating consequences for the site and its surrounding communities. Because of these risks, DOE needs an effective safeguards and security program. A key component of an effective program is the design basis threat (DBT), a classified document that identifies, among other things, the potential size and capabilities of terrorist forces. The terrorist attacks of September 11, 2001, rendered the then-current DBT obsolete, resulting in DOE issuing a new version in May 2003.

GAO (1) identified why DOE took almost 2 years to develop a new DBT, (2) analyzed the higher threat in the new DBT, and (3) identified remaining issues that need to be resolved in order for DOE to meet the threat contained in the new DBT.

www.gao.gov/cgi-bin/getrpt?GAO-04-701T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robin M. Nazzaro at (202) 512-3841 or nazzaror@gao.gov.

April 27, 2004

NUCLEAR SECURITY

DOE Must Address Significant Issues to Meet the Requirements of the New Design Basis Threat

What GAO Found

DOE took a series of actions in response to the terrorist attacks of September 11, 2001. While each of these has been important, in and of themselves, they are not sufficient to ensure that all of DOE's sites are adequately prepared to defend themselves against the higher terrorist threat present in the post September 11, 2001 world. Specifically, GAO found:

- DOE took almost 2 years to develop a new DBT because of (1) delays in developing an intelligence community assessment—known as the Postulated Threat—of the terrorist threat to nuclear weapon facilities, (2) DOE's lengthy comment and review process for developing policy, and (3) sharp debates within DOE and other government organizations over the size and capabilities of future terrorist threats and the availability of resources to meet these threats.

- While the May 2003 DBT identifies a larger terrorist threat than did the previous DBT, the threat identified in the new DBT, in most cases, is less than the threat identified in the intelligence community's Postulated Threat, on which the DBT has been traditionally based. The new DBT identifies new possible terrorist acts such as radiological, chemical, or biological sabotage. However, the criteria that DOE has selected for determining when facilities may need to be protected against these forms of sabotage may not be sufficient. For example, for chemical sabotage, the 2003 DBT requires sites to protect to "industry standards;" however, such standards currently do not exist.

- DOE has been slow to resolve a number of significant issues, such as issuing additional DBT implementation guidance, developing DBT implementation plans, and developing budgets to support these plans, that may affect the ability of its sites to fully meet the threat contained in the new DBT in a timely fashion. Consequently, DOE's deadline to meet the requirements of the new DBT by the end of fiscal year 2006 is probably not realistic for some sites.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our work for this Subcommittee on physical security at the Department of Energy (DOE) and the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE. Specifically, today we are issuing our report, *Nuclear Security: DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat* (GAO-04-623).

DOE has long recognized that a successful terrorist attack on a site containing nuclear weapons or the material used in nuclear weapons—called special nuclear material—could have devastating consequences for the site and its surrounding communities. Because terrorist attacks against sites that contain special nuclear material could have such devastating consequences, DOE's effective management of the safeguards and security program, which includes developing safeguards and security policies, is essential to preventing an unacceptable, adverse impact on national security.[1] For many years, DOE has employed risk-based security practices. To manage potential risks, DOE has developed a design basis threat (DBT), a classified document that identifies the potential size and capabilities of terrorist forces. DOE's DBT is based on an intelligence community assessment known as the Postulated Threat. DOE requires the contractors operating its sites to provide sufficient protective forces and equipment to defend against the threat contained in the DBT. The DBT in effect on September 11, 2001, had been DOE policy since June 1999. DOE replaced the 1999 DBT in May 2003 to better reflect the current and projected terrorist threats that resulted from the September 11, 2001, attacks.

Following the September 11, 2001, terrorist attacks, you asked us to review physical security at DOE sites that have facilities with Category I special nuclear material. Category I special nuclear material includes specified quantities of plutonium and highly enriched uranium in forms of assembled nuclear weapons and test devices, major nuclear components, and other high-grade materials such as solutions and oxides. Specifically, we examined, among other things, (1) the reasons DOE needed almost 2 years to develop a new DBT; (2) the higher threat contained in the new

[1]See U.S. General Accounting Office, *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471 (Washington, D.C.: May 30, 2003).

DBT; and (3) the remaining issues that need to be resolved in order for DOE to fully defend against the threat contained in the new DBT.[2]

To carry out our objectives, we reviewed draft DBTs, the final May 2003 DBT, and DOE policy and planning documents, including orders, implementation guidance, and reports. We met with officials from DOE and NNSA headquarters and field offices. We obtained information primarily from DOE's Office of Security, Office of Independent Oversight and Performance Assurance, and Office of Environmental Management; NNSA's Office of Defense Nuclear Security; and NNSA's Nuclear Safeguards and Security Program. We visited all three of NNSA's three design laboratories and its two production plants that possess Category I special nuclear material, as well as NNSA's Office of Secure Transportation. We also visited the four EM sites that, at the time, contained Category I special nuclear materials. At each site we met with both federal and contractor officials and reviewed pertinent supporting documentation. We also discussed postulated terrorist threats to nuclear weapon facilities with two Department of Defense (DOD) organizations: the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; and the Defense Intelligence Agency. We also reviewed *The Postulated Threat to U.S. Nuclear Weapon Facilities and Other Selected Strategic Facilities*, henceforth referred to as the Postulated Threat, which is the intelligence community's January 2003 official assessment of potential terrorist threats to nuclear weapon facilities.

We performed our work from December 2001 through April 2004 in accordance with generally accepted government auditing standards.

In summary, we found that while DOE has taken some important actions in its response to the terrorist attacks of September 11, 2001, DOE struggled to develop its new DBT. The DBT that DOE ultimately developed, however, is substantially more demanding than the previous one. Because the new DBT is more demanding and because DOE wants to implement new protective strategies within 2 years, DOE must press forward with additional actions to ensure that it is fully prepared to

[2]We testified on these issues before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform, on June 24, 2003. See U.S. General Accounting Office, *Nuclear Security: DOE's Response to the September 11, 2001 Terrorist Attacks*, GAO-03-898TC (Washington, D.C.: June 24, 2003).

provide a timely and cost effective defense of its most sensitive facilities. Specifically, we found the following:

- Development of the new DBT took almost 2 years because of (1) delays in developing an intelligence community assessment—known as the Postulated Threat—of the terrorist threat to nuclear weapon facilities, (2) DOE's lengthy comment and review process for developing policy, and (3) sharp debates within DOE and other government organizations over the size and capabilities of future terrorist threats and the availability of resources to meet these threats.

- While the May 2003 DBT identifies a larger terrorist threat than did the previous DBT, the threat identified in the new DBT, in most cases, is less than the threat identified in the intelligence community's Postulated Threat, on which the DBT has been traditionally based. The new DBT identifies new possible terrorist acts such as radiological, chemical, or biological sabotage. However, the criteria that DOE has selected for determining when facilities may need to be protected against these forms of sabotage may not be sufficient. For example, for chemical sabotage, the 2003 DBT requires sites to protect to "industry standards;" however, such standards currently do not exist.

- DOE has been slow to resolve a number of significant issues, such as issuing additional DBT implementation guidance, developing DBT implementation plans, and developing budgets to support these plans, that may affect the ability of its sites to fully meet the threat contained in the new DBT in a timely fashion. Consequently, DOE's deadline to meet the requirements of the new DBT by the end of fiscal year 2006 is probably not realistic for some sites.

In our report to you, we made seven recommendations to the Secretary of Energy that are intended to strengthen DOE's ability to meet the requirements of the new DBT, improve the department's ability to deal with future terrorist threats, and better inform Congress on departmental progress in meeting the threat contained in the new DBT and reducing risks to critical facilities at DOE sites. DOE did not comment specifically on our recommendations other than to say that the department would consider them as part of its Departmental Management Challenges for 2004. DOE has identified the DBT as a major departmental initiative within the National Security Management Challenge.

Background

Category I special nuclear materials are present at the three design laboratories—the Los Alamos National Laboratory in Los Alamos, New

Mexico; the Lawrence Livermore National Laboratory in Livermore, California; and the Sandia National Laboratory in Albuquerque, New Mexico—and two production sites—the Pantex Plant in Amarillo, Texas, and the Y-12 Plant in Oak Ridge, Tennessee, operated by NNSA. Special nuclear material is also present at former production sites, including the Savannah River Site in Savannah River, South Carolina, and the Hanford Site in Richland, Washington. These former sites are now being cleaned up by DOE's Office of Environmental Management (EM).[3] Furthermore, NNSA's Office of Secure Transportation transports these materials among the sites and between the sites and DOD bases. Contractors operate each site for DOE.[4] NNSA and EM have field offices collocated with each site. In fiscal year 2004, NNSA and EM expect to spend nearly $900 million on physical security at their sites.[5] Physical security combines security equipment, personnel, and procedures to protect facilities, information, documents, or material against theft, sabotage, diversion, or other criminal acts.

In addition to NNSA and EM, DOE has other important security organizations. DOE's Office of Security develops and promulgates orders and policies, such as the DBT, to guide the department's safeguards and security programs. DOE's Office of Independent Oversight and Performance Assurance supports the department by, among other things, independently evaluating the effectiveness of contractors' performance in safeguards and security. It also performs follow-up reviews to ensure that contractors have taken effective corrective actions and appropriately addressed weaknesses in safeguards and security. Under a recent reorganization, these two offices were incorporated into the new Office of Security and Safety Performance Assurance. Each office, however, retains its individual missions, functions, structure, and relationship to the other.

[3]At the time of our review, the Rocky Flats Environmental Technology Site in Rocky Flats, Colorado, was in the process of shipping its remaining Category I special nuclear material primarily to the Savannah River Site. This has now been completed. In addition, responsibility for the Idaho National Engineering and Environmental Laboratory, in Idaho Falls, Idaho, which is also a Category I special nuclear material site, was transferred from DOE's EM to DOE's Office of Nuclear Energy in May 2003.

[4]Federal employees instead of contractors operate the assets of the Office of Secure Transportation.

[5]Other DOE program offices, such as the Office of Science and Office of Nuclear Energy operate sites that may contain Category I special nuclear material. In fiscal year 2004, these program offices expect to spend $118 million on security.

The risks associated with Category I special nuclear materials vary but include the nuclear detonation of a weapon or test device at or near design yield, the creation of improvised nuclear devices capable of producing a nuclear yield, theft for use in an illegal nuclear weapon, and the potential for sabotage in the form of radioactive dispersal. Because of these risks, DOE has long employed risk-based security practices.

The key component of DOE's well-established, risk-based security practices is the DBT, a classified document that identifies the characteristics of the potential threats to DOE assets. The DBT has been traditionally based on a classified, multiagency intelligence community assessment of potential terrorist threats, known as the Postulated Threat. The DBT considers a variety of threats in addition to the terrorist threat. Other adversaries considered in the DBT include criminals, psychotics, disgruntled employees, violent activists, and spies. The DBT also considers the threat posed by insiders, those individuals who have authorized, unescorted access to any part of DOE facilities and programs. Insiders may operate alone or may assist an adversary group. Insiders are routinely considered to provide assistance to the terrorist groups found in the DBT. The threat from terrorist groups is generally the most demanding threat contained in the DBT.

DOE counters the terrorist threat specified in the DBT with a multifaceted protective system. While specific measures vary from site to site, all protective systems at DOE's most sensitive sites employ a defense-in-depth concept that includes sensors, physical barriers, hardened facilities and vaults, and heavily armed paramilitary protective forces equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear.

Depending on the material, protective systems at DOE Category I special nuclear material sites are designed to accomplish the following objectives in response to the terrorist threat:

- *Denial of access.* For some potential terrorist objectives, such as the creation of an improvised nuclear device, DOE may employ a protection strategy that requires the engagement and neutralization of adversaries before they can acquire hands-on access to the assets.

- *Denial of task.* For nuclear weapons or nuclear test devices that terrorists might seek to steal, DOE requires the prevention and/or neutralization of

the adversaries before they can complete a specific task, such as stealing such devices.

- *Containment with recapture.* Where the theft of nuclear material (instead of a nuclear weapon) is the likely terrorist objective, DOE requires that adversaries not be allowed to escape the facility and that DOE protective forces recapture the material as soon as possible. This objective requires the use of specially trained and well-equipped special response teams.

The effectiveness of the protective system is formally and regularly examined through vulnerability assessments. A vulnerability assessment is a systematic evaluation process in which qualitative and quantitative techniques are applied to detect vulnerabilities and arrive at effective protection of specific assets, such as special nuclear material. To conduct such assessments, DOE uses, among other things, subject matter experts, such as U.S. Special Forces; computer modeling to simulate attacks; and force-on-force performance testing, in which the site's protective forces undergo simulated attacks by a group of mock terrorists.

The results of these assessments are documented at each site in a classified document known as the Site Safeguards and Security Plan. In addition to identifying known vulnerabilities, risks, and protection strategies for the site, the Site Safeguards and Security Plan formally acknowledges how much risk the contractor and DOE are willing to accept. Specifically, for more than a decade, DOE has employed a risk management approach that seeks to direct resources to its most critical assets—in this case Category I special nuclear material—and mitigate the risks to these assets to an acceptable level. Levels of risk—high, medium, and low—are assigned classified numerical values and are derived from a mathematical equation that compares a terrorist group's capabilities with the overall effectiveness of the crucial elements of the site's protective forces and systems.

Historically, DOE has striven to keep its most critical assets at a low risk level and may insist on immediate compensatory measures should a significant vulnerability develop that increases risk above the low risk level. Compensatory measures could include such things as deploying additional protective forces or curtailing operations until the asset can be better protected. In response to a September 2000 DOE Inspector General's report recommending that DOE establish a policy on what actions are required once high or moderate risk is identified, in September 2003, DOE's Office of Security issued a policy clarification stating that identified high risks at facilities must be formally reported to the Secretary

of Energy or Deputy Secretary within 24 hours. In addition, under this policy clarification, identified high and moderate risks require corrective actions and regular reporting.

Through a variety of complementary measures, DOE ensures that its safeguards and security policies are being complied with and are performing as intended. Contractors perform regular self-assessments and are encouraged to uncover any problems themselves. DOE Orders also require field offices to comprehensively survey contractors' operations for safeguards and security every year. DOE's Office of Independent Oversight and Performance Assurance provides yet another check through its comprehensive inspection program. All deficiencies identified during surveys and inspections require the contractors to take corrective action.

Development of the New DBT Took Almost 2 Years Because of Delays in Developing the Postulated Threat and DOE's Lengthy Review and Comment Process

In the immediate aftermath of September 11, 2001, DOE officials realized that the then current DBT, issued in April 1999 and based on a 1998 intelligence community assessment, was obsolete. The September 11, 2001, terrorist attacks suggested larger groups of terrorists, larger vehicle bombs, and broader terrorist aspirations to cause mass casualties and panic than were envisioned in the 1999 DOE DBT. However, formally recognizing these new threats by updating the DBT was difficult and took 21 months because of delays in issuing the Postulated Threat, debates over the size of the future threat and the cost to meet it, and the DOE policy process.

As mentioned previously, DOE's new DBT is based on a study known as the Postulated Threat, which was developed by the U.S. intelligence community. The intelligence community originally planned to complete the Postulated Threat by April 2002; however, the document was not completed and officially released until January 2003, about 9 months behind the original schedule. According to DOE and DOD officials, this delay resulted from other demands placed on the intelligence community after September 11, 2001, as well as from sharp debates among the organizations developing the Postulated Threat over the size and capabilities of future terrorist threats and the resources needed to meet these threats.

While waiting for the new Postulated Threat, DOE developed several drafts of its new DBT. During this process, debates, similar to those that occurred during the development of the Postulated Threat, emerged in DOE. Like the participants responsible for developing the Postulated Threat, during the development of the DBT, DOE officials debated the size

of the future terrorist threat and the costs to meet it. DOE officials at all levels told us that concern over resources played a large role in developing the 2003 DBT, with some officials calling the DBT the "funding basis threat," or the maximum threat the department could afford. This tension between threat size and resources is not a new development. According to a DOE analysis of the development of prior DBTs, political and budgetary pressures and the apparent desire to reduce the requirements for the size of protective forces appear to have played a significant role in determining the terrorist group numbers contained in prior DBTs.

Finally, DOE developed the DBT using DOE's policy process, which emphasizes developing consensus through a review and comment process by program offices, such as EM and NNSA. However, many DOE and contractor officials found that the policy process for developing the new DBT was laborious and not timely, especially given the more dangerous threat environment that has existed since September 11, 2001. As a result, during the time it took DOE to develop the new DBT, its sites were only required to defend against the terrorist group defined in the 1999 DBT, which, in the aftermath of September 11, 2001, DOE officials realized was obsolete.

The May 2003 DBT Identifies a Larger Terrorist Threat, but in Most Cases is Less Than the Terrorist Threat Identified by the Postulated Threat

While the May 2003 DBT identifies a larger terrorist group than did the previous DBT, the threat identified in the new DBT, in most cases, is less than the terrorist threat identified in the intelligence community's Postulated Threat. The Postulated Threat estimated that the force attacking a nuclear weapons site would probably be a relatively small group of terrorists, although it was possible that an adversary might use a greater number of terrorists if that was the only way to attain an important strategic goal. In contrast to the Postulated Threat, DOE is preparing to defend against a significantly smaller group of terrorists attacking many of its facilities. Specifically, only for its sites and operations that handle nuclear weapons is DOE currently preparing to defend against an attacking force that approximates the lower range of the threat identified in the Postulated Threat. For its other Category I special nuclear material sites, all of which fall under the Postulated Threat's definition of a nuclear weapons site, DOE is requiring preparations to defend against a terrorist force significantly smaller than was identified in the Postulated Threat. DOE calls this a graded threat approach.

Some of these other sites, however, may have improvised nuclear device concerns that, if successfully exploited by terrorists, could result in a nuclear detonation. Nevertheless, under the graded threat approach, DOE

requires these sites only to be prepared to defend against a smaller force of terrorists than was identified by the Postulated Threat. Officials in DOE's Office of Independent Oversight and Performance Assurance disagreed with this approach and noted that sites with improvised nuclear device concerns should be held to the same requirements as facilities that possess nuclear weapons and test devices since the potential worst-case consequence at both types of facilities would be the same—a nuclear detonation. Other DOE officials and an official in DOD's Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence disagreed with the overall graded threat approach, believing that the threat should not be embedded in the DBT by adjusting the number of terrorists that might attack a particular target.

DOE Office of Security officials cited three reasons for why the department departed from the Postulated Threat's assessment of the potential size of terrorist forces. First, these officials stated that they believed that the Postulated Threat only applied to sites that handled completed nuclear weapons and test devices. However, both the 2003 Postulated Threat, as well as the preceding 1998 Postulated Threat, state that the threat applies to nuclear weapons and special nuclear material without making any distinction between them. Second, DOE Office of Security officials believed that the higher threat levels contained in the 2003 Postulated Threat represented the worst potential worldwide terrorist case over a 10-year period. These officials noted that while some U.S. assets, such as military bases, are located in parts of the world where terrorist groups receive some support from local governments and societies thereby allowing for an expanded range of capabilities, DOE facilities are located within the United States, where terrorists would have a more difficult time operating. Furthermore, DOE Office of Security officials stated that the DBT focuses on a nearer-term threat of 5 years. As such, DOE Office of Security officials said that they chose to focus on what their subject matter experts believed was the maximum, credible, near-term threat to their facilities. However, while the 1998 Postulated Threat made a distinction between the size of terrorist threats abroad and those within the United States, the 2003 Postulated Threat, reflecting the potential implications of the September 2001 terrorist attacks, did not make this distinction. Finally, DOE Office of Security officials stated that the Postulated Threat document represented a reference guide instead of a policy document that had to be rigidly followed. The Postulated Threat does acknowledge that it should not be used as the sole consideration to dictate specific security requirements and that decisions regarding security risks should be made and managed by decision makers in policy offices. However, DOE has traditionally based its DBT on the Postulated

Threat. For example, the prior DBT, issued in 1999, adopted exactly the same terrorist threat size as was identified by the 1998 Postulated Threat.

Finally, the department's criteria for determining the severity of radiological, chemical, and biological sabotage may be insufficient. For example, the criterion used for protection against radiological sabotage is based on acute radiation dosages received by individuals. However, this criterion may not fully capture or characterize the damage that a major radiological dispersal at a DOE site might cause. For example, according to a March 2002 DOE response to a January 23, 2002, letter from Representative Edward J. Markey, a worst-case analysis at one DOE site showed that while a radiological dispersal would not pose immediate, acute health problems for the general public, the public could experience measurable increases in cancer mortality over a period of decades after such an event. Moreover, releases at the site could also have environmental consequences requiring hundreds of millions to billions of dollars to clean up. Contamination could also affect habitability for tens of miles from the site, possibly affecting hundreds of thousands of residents for many years. Likewise, the same response showed that a similar event at a NNSA site could result in a dispersal of plutonium that could contaminate several hundred square miles and ultimately cause thousands of cancer deaths. For chemical sabotage standards, the 2003 DBT requires sites to protect to industry standards. However, we reported March 2003 year that such standards currently do not exist.[6] Specifically, we found that no federal laws explicitly require chemical facilities to assess vulnerabilities or take security actions to safeguard their facilities against a terrorist attack. Finally, the protection criteria for biological sabotage are based on laboratory safety standards developed by the U.S. Centers for Disease Control and not physical security standards.

[6]See U.S. General Accounting Office, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439 (Washington, D.C.: Mar. 14, 2003).

DOE Has Been Slow to Resolve a Number of Significant Issues That May Affect the Ability of its Sites to Fully Meet the Threat Contained in the New DBT

While DOE issued the final DBT in May 2003, it has only recently resolved a number of significant issues that may affect the ability of its sites to fully meet the threat contained in the new DBT in a timely fashion and is still addressing other issues. Fully resolving all of these issues may take several years, and the total cost of meeting the new threats is currently unknown. Because some sites will be unable to effectively counter the higher threat contained in the new DBT for up to several years, these sites should be considered to be at higher risk under the new DBT than they were under the old DBT.

In order to undertake the necessary range of vulnerability assessments to accurately evaluate their level of risk under the new DBT and implement necessary protective measures, DOE recognized that it had to complete a number of key activities. DOE only recently completed three of these key activities. First, in February 2004, DOE issued its revised Adversary Capabilities List, which is a classified companion document to the DBT, that lists the potential weaponry, tactics, and capabilities of the terrorist group described in the DBT. This document has been amended to include, among other things, heavier weaponry and other capabilities that are potentially available to terrorists who might attack DOE facilities. DOE is continuing to review relevant intelligence information for possible incorporation into future revisions of the Adversary Capabilities List.

Second, DOE also only recently provided additional DBT implementation guidance. In a July 2003 report, DOE's Office of Independent Oversight and Performance Assurance noted that DOE sites had found initial DBT implementation guidance confusing. For example, when the Deputy Secretary of Energy issued the new DBT in May 2003, the cover memo said the new DBT was effective immediately but that much of the DBT would be implemented in fiscal years 2005 and 2006. According to a 2003 report by the Office of Independent Oversight and Performance Assurance, many DOE sites interpreted this implementation period to mean that they should, through fiscal year 2006, only be measured against the previous, less demanding 1999 DBT.

In response to this confusion, the Deputy Secretary issued further guidance in September 2003 that called for the following, among other things:

- DOE's Office of Security to issue more specific guidance by October 22, 2003, regarding DBT implementation expectations, schedules, and requirements. DOE issued this guidance January 30, 2004.

- Quarterly reports showing sites' incremental progress in meeting the new DBT for ongoing activities. The first series of quarterly progress reports may be issued in July 2004.

- Immediate compliance with the new DBT for new and reactivated operations.

A third important DBT-related issue was just completed in early April 2004. A special team created in the 2003 DBT, composed of weapons designers and security specialists, finalized its report on each site's improvised nuclear device vulnerabilities. The results of this report were briefed to senior DOE officials in March 2004 and the Deputy Secretary of Energy issued guidance, based on this report, to DOE sites in early April 2004. As a result, some sites may be required under the 2003 DBT to shift to enhanced protection strategies, which could be very costly. This special team's report may most affect EM sites because their improvised nuclear device potential had not previously been explored.

Finally, DOE's Office of Security has not completed all of the activities associated with the new vulnerability assessment methodology it has been developing for over a year. DOE's Office of Security believes this methodology, which uses a new mathematical equation for determining levels of risk, will result in a more sensitive and accurate portrayal of each site's defenses-in-depth and the effectiveness of sites' protective systems (i.e., physical security systems and protective forces) when compared with the new DBT. DOE's Office of Security decided to develop this new equation because its old mathematical equation had been challenged on technical grounds and did not give sites credit for the full range of their defenses-in-depth. While DOE's Office of Security completed this equation in December 2002, officials from this office believe it will probably not be completely implemented at the sites for at least another year for two reasons. First, site personnel who implement this methodology will require additional training to ensure they are employing it properly. DOE's Office of Security conducted initial training in December 2003, as well as a prototype course in February 2004, and has developed a nine-course vulnerability assessment certification program. Second, sites will have to collect additional data to support the broader evaluation of their protective systems against the new DBT. Collecting these data will require additional computer modeling and force-on-force performance testing.

Because of the slow resolution of some of these issues, DOE has not developed any official long-range cost estimates or developed any integrated, long-range implementation plans for the May 2003 DBT.

Specifically, neither the fiscal year 2003 nor 2004 budgets contained any provisions for DBT implementation costs. However, during this period, DOE did receive additional safeguards and security funding through budget reprogramming and supplemental appropriations. DOE is using most of these additional funds to cover the higher operational costs associated with the increased security condition (SECON) measures. DOE has gathered initial DBT implementation budget data and has requested additional DBT implementation funding in the fiscal year 2005 budget: $90 million for NNSA, $18 million for the Secure Transportation Asset within the Office of Secure Transportation, and $26 million for EM. However, DOE officials believe the budget data collected so far has been of generally poor quality because most sites have not yet completed the necessary vulnerability assessments to determine their resource requirements. Consequently, the fiscal year 2006 budget may be the first budget to begin to accurately reflect the safeguards and security costs of meeting the requirements of the new DBT.

Reflecting these various delays and uncertainties, in September 2003, the Deputy Secretary changed the deadline for DOE program offices, such as EM and NNSA, to submit DBT implementation plans from the original target of October 2003 to the end of January 2004. NNSA and EM approved these plans in February 2004. DOE's Office of Security has reviewed these plans and is planning to provide implementation assistance to sites that request it. DOE officials have described these plans as being ambitious in terms of the amount of work that has to be done within a relatively short time frame and dependent on continued increases in safeguards and security funding, primarily for additional protective force personnel. However, some plans may be based on assumptions that are no longer valid. Revising these plans could require additional resources, as well as add time to the DBT implementation process.

A DOE Office of Budget official told us that current DBT implementation cost estimates do not include items such as closing unneeded facilities, transporting and consolidating materials, completing line item construction projects, and other important activities that are outside of the responsibility of the safeguards and security program. For example, EM's Security Director told us that for EM to fully comply with the DBT requirements in fiscal year 2006 at one of its sites, it will have to

- close and de-inventory two facilities,
- consolidate excess materials into remaining special nuclear materials facilities, and

- move consolidated Category I special nuclear material, which NNSA's Office of Secure Transportation will transport, to another site.

Likewise, the EM Security Director told us that to meet the DBT requirements at another site, EM will have to accelerate the closure of one facility and transfer special nuclear material to another facility on the site. The costs to close these facilities and to move materials within a site are borne by the EM program budget and not by the EM safeguards and security budget. Similarly, the costs to transport the material between sites are borne by NNSA's Office of Secure Transportation budget and not by EM's safeguards and security budget. A DOE Office of Budget official told us that a comprehensive, department-wide approach to budgeting for DBT implementation that includes such important program activities as described above is needed; however, such an approach does not currently exist.

The department plans to complete DBT implementation by the end of fiscal year 2006. However, most sites estimate that it will take 2 to 5 years, if they receive adequate funding, to fully meet the requirements of the new DBT. During this time, sites will have to conduct vulnerability assessments, undertake performance testing, and develop Site Safeguards and Security Plans. Consequently, full DBT implementation could occur anywhere from fiscal year 2005 to fiscal year 2008. Some sites may be able to move more quickly and meet the department's deadline of the end of fiscal year 2006.

Because some sites will be unable to effectively counter the threat contained in the new DBT for a period of up to several years, these sites should be considered to be at higher risk under the new DBT than they were under the old DBT. For example, the Office of Independent Oversight and Performance Assurance has concluded in recent inspections that at least two DOE sites face fundamental and not easily resolved security problems that will make meeting the requirements of the new DBT difficult. For other DOE sites, their level of risk under the new DBT remains largely unknown until they can conduct the necessary vulnerability assessments.

In closing, while DOE struggled to develop its new DBT, the DBT that DOE ultimately developed is substantially more demanding than the previous one. Because the new DBT is more demanding and because DOE wants to implement it by end of fiscal year 2006—a period of about 29 months—DOE must press forward with a series of additional actions to

ensure that it is fully prepared to provide a timely and cost effective defense of its most sensitive facilities.

First, because the September 11, 2001, terrorist attacks suggested larger groups of terrorists with broader aspirations for causing mass casualties and panic, we believe that the DBT development process that was used requires reexamination. While DOE may point to delays in the development of the Postulated Threat as the primary reason for the almost 2 years it took to develop a new DBT, DOE was also working on the DBT itself for most of that time. We believe the difficulty associated with developing a consensus using DOE's traditional policy-making process was a key factor in the time it took to develop a new DBT. During this extended period, DOE's sites were only being defended against what was widely recognized as an obsolete terrorist threat level.

Second, we are concerned about two aspects of the resulting DBT. We are not persuaded that there is sufficient difference, in its ability to achieve the objective of causing mass casualties or creating public panic, between the detonation of an improvised nuclear device and the detonation of a nuclear weapon or test device at or near design yield that warrants setting the threat level at a lower number of terrorists. Furthermore, while we applaud DOE for adding additional requirements to the DBT such as protection strategies to guard against radiological, chemical, and biological sabotage, we believe that DOE needs to reevaluate its criteria for terrorist acts of sabotage, especially in the chemical area, to make it more defensible from a physical security perspective.

Finally, because some sites will be unable to effectively counter the threat contained in the new DBT for a period of up to several years, these sites should be considered to be at higher risk under the new DBT than they were under the old DBT. As a result, DOE needs to take a series of actions to mitigate these risks to an acceptable level as quickly as possible. To accomplish this, it is important for DOE to go about the hard business of a comprehensive department-wide approach to implementing needed changes in its protective strategy. Because the consequences of a successful terrorist attack on a DOE site could be so devastating, we believe it is important for DOE to better inform Congress about what sites are at high risk and what progress is being made to reduce these risks to acceptable levels.

Mr. Chairman, this concludes our prepared statement. We would be happy to respond to any questions that you or Members of the Subcommittee may have.

GAO Contact and Staff Acknowledgments

For further information on this testimony, please contact Robin M. Nazzaro at (202) 512-3841. James Noel and Jonathan Gill also made key contributions to this testimony.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

Mr. SHAYS. Thank you very much.

Ms. Brian, would you just explain what your organization is for the record?

Ms. BRIAN. Yes. We are an independent nonprofit government watchdog organization.

Mr. SHAYS. Thank you.

And at this time I would want to just thank the Administrator Linton Brooks and Glenn Podonsky, because they could have asked to go first. And I think it's important that the concern be expressed and then have them be able to respond to it. So it's logical to have them follow.

But I just want, Ms. Brian, for you to know that you are able to speak first because they have agreed to it. And I thank them for that.

And it's very nice to have you here.

Ms. BRIAN. And I thank you for having me here as well, chairman.

If you could please enter my written testimony in the record.

Mr. SHAYS. That will be done.

Ms. BRIAN. POGO is heartened that this committee has remained so active in overseeing the nuclear weapons complex and its ongoing security challenges.

I must say, at your previous hearing, though, I was relatively pessimistic that we would ever be successful in gaining any real security improvements from DOE. Since then, however, POGO has become more guardedly optimistic.

We had the opportunity to meet with Secretary Abraham, Deputy Secretary McSlarrow, and SSA Director Podonsky this January.

We began in that meeting ongoing communication with the Secretary regarding our concerns and recommendations. We have reason to believe he is taking these issues seriously. Our best evidence of that is the recent announcement that Los Alamos' TA–18 is finally going to be deinventoried of its special nuclear materials.

Mr. SHAYS. You can slow down just a little bit. You can run over 5 minutes.

Ms. BRIAN. I can? OK. Thank you.

Furthermore, the new design basis threat and requirement that all Category I sites be able to prevent terrorists from even entering the facility will require major changes in defensive strategies and upgraded infrastructure.

In the face of these requirements, these sites can no longer apply Band-Aids to the security problems. DOE simply no longer has the luxury of having SNM, special nuclear materials, at sites that can't be adequately protected or where the costs of protection are prohibitive. This is a critical turning point in the direction of the nuclear weapons complex.

The Department has to immediately begin to deinventory certain sites, transferring the SNM to more secure sites; build underground storage facilities at Savannah River and Y–12; and blend down the excess highly enriched uranium and immobilize the excess plutonium. These steps would make the nuclear materials far less attractive to terrorists.

In addition to highlighting the urgent need to move the SNM from TA–18, we raised several other priorities for the Secretary's consideration. This winter, POGO began focusing on security at two additional NNSA sites, Lawrence Livermore National Lab just east of San Francisco, and the Y–12 plant in Oak Ridge, TN. Both face serious physical security challenges, perhaps insurmountable challenges.

We don't feel comfortable discussing publicly the specific concerns we have regarding Livermore security. However, we can say that the encroaching residential community surrounding Livermore has made it nearly impossible to properly protect the SNM stored there. Clearly, they will not be able to comply with the new directives.

In light of this facility's vulnerabilities, POGO recommends that all SNMs be deinventoried from Livermore immediately and sent to the Nevada test site. This move would dramatically increase security while saving about $30 million in annual security costs.

Some in DOE and the Congress have identified Y–12 as the most serious security concern in the complex. Y–12 stores hundreds of tons of highly enriched uranium and is a prime target for terrorists who would want to create an improvised nuclear devise within minutes. Given the obsolete infrastructure currently housing the highly enriched uranium, it should come as no surprise that the Y–12 guard force has been systemically cheating in order to pass security performance tests. They simply cannot protect the material in the six material access areas given the multiple targets, dilapidated infrastructure, and very short timelines for the terrorists to reach their target.

The current contractor operating Y–12, BWXT, inexplicably changed a plan to build a bermed facility that would be covered by earth on three sides and its roof and is now planning to build an above-ground facility. However, the IG has concluded that the new design for the storage facility will actually decrease security and increase costs significantly.

Immediate funding for underground storage at Y–12 and the blending down of the over 100 tons of excess highly enriched uranium should be the top priorities of the NNSA budget.

There have also been significant security problems at Sandia National Lab in Albuquerque, NM. The only weapons quantities of SNM stored at Sandia are the highly enriched uranium fuel plates for the SPR-III burst reactor. This reactor is rarely used. Moving this reactor and its fuel to the Nevada test site again would dramatically reduce security requirements and save about $30 million annually in security costs.

In addition, the Idaho facilities store tons of SNM, the second largest repository of highly enriched uranium in the complex. These nuclear materials are left over from the cold war and abandoned research projects. They have no current national defense mission. These facilities should also be deinventoried of weapons quantities SNM.

POGO sources have suggested that the DBT at most sites remains inadequate as, of course, the GAO is testifying today, far below the level of security recommended by the intelligence com-

munity, particularly at sites with improvised nuclear device vulnerabilities.

As the GAO pointed out in its report presented at your last hearing, the DBT was, of course, cost-driven. The GAO wrote, "Some officials called the DBT the funding basis threat, or the maximum threat the Department could afford." As you said in your testimony, this is not an acceptable method for determining security standards. The DBT should be reevaluated to bring it more in line with the realistic threat contained in the intelligence community's postulated threat, particularly for IND vulnerable sites.

A final note regarding the TA–18 move. POGO is concerned that there are people in the complex who are still trying to sabotage this move. While POGO was heartened by the original announcement regarding the move, our hopes were dampened after meeting with the head of the nuclear weapons complex, Dr. Everet Beckner. Despite Secretary Abraham's intentions that all Category I special nuclear materials should be out of TA–18 by 2005, Dr. Beckner informed us that NNSA only intends to move 50 percent of it. I have provided to your staff a memo that confirms this is his intention.

[The information referred to follows:]

Department of Energy
National Nuclear Security Administration
Washington, DC 20585
April 9, 2004

TO Manager, Livermore Site Office
Manager, Los Alamos Site Office
Manager, Nevada Site Office
Director, Lawrence Livermore National Laboratory
Director, Los Alamos National Laboratory
Manager, Bechtel Nevada

FROM Everet H Beckner
Deputy Administrator for Defense Programs

SUBJECT Los Alamos Technical Area 18 (TA-18) Mission Relocation

On March 31, 2004, the National Nuclear Security Administration (NNSA) announced an initiative to begin moving Special Nuclear Materials (SNM) from TA-18 to the Device Assembly Facility (DAF) at the Nevada Test Site (NTS) Beginning in September 2004, NNSA will ship about 50 percent of the entire TA-18 programmatic SNM inventory to the DAF during an 18-month period Based on this decision, the following direction is provided regarding the early move of TA-18 SNM and the TA-18 Mission Relocation Project

First, the early move of TA-18 SNM to the DAF will occur separately from the TA-18 Mission Relocation Project The Nevada Site Office (NSO) will work with the Livermore Site Office, Lawrence Livermore National Laboratory (LLNL), and Bechtel Nevada to start preparing the DAF to support staging of SNM immediately, while the NNSA coordinates packaging and transportation activities Additionally, the NSO will direct Wackenhut Security Incorporated to initiate hiring processes to increase the DAF security posture Within 30 days, the NSO will provide a resource-loaded plan, including funding requirements, for NNSA approval

Second, NNSA, along with the Los Alamos National Laboratory (LANL), will assess the entire TA-18 security category I/II inventory and prepare a detailed plan to support the initial shipment of SNM to the DAF The goal is to develop a plan for a smooth shipping schedule in accordance with the 18-month schedule, utilizing existing shipping containers to the extent practical

Ms. BRIAN. In a separate meeting, Ambassador Brooks told us that moving only part of the material would not improve security at all. This is, of course, because enough material would remain behind to still create an improvised nuclear device.

Dr. Beckner went on to inform us that the ballooning cost for this move from $100 million to $300 million was in large part, a result of the requirement to produce authorization basis documents to move the burst reactors from Los Alamos and to operate them at the Nevada test site. He told us this paperwork requirement alone would cost $150 million. We checked with the person in the Los Alamos area office who is responsible for signing off on such documents. He estimated the cost to be between $1 and $2 million if done correctly, and as much as $6 million on the outside if it needs to be reworked.

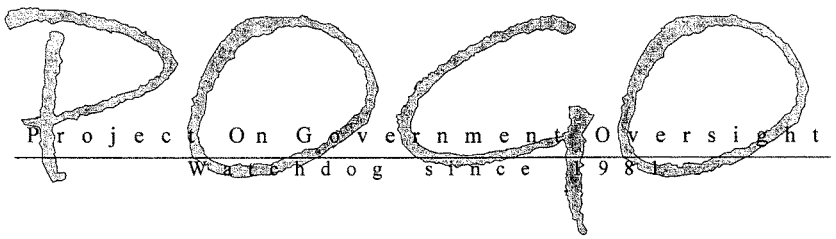
I am raising this to illustrate how the bureaucracy knowingly provides baseless information to headquarters as a way of protecting the status quo. It is essential that the committee straighten out this confusion today during this hearing.

POGO is guardedly optimistic that Secretary Abraham and Deputy Secretary McSlarrow are sincerely concerned about the state of security at the nuclear weapons complex. However, these officials have a limited time in office.

The Office of Security and Safety Performance Assurance will be the entity left behind to oversee any improvements. This office is doing extremely important work, but their limitation is that they do not have either the necessary independence or power to see this difficult job done correctly.

Congress needs to formalize its communications with this office as it has with the Inspector General. Your ongoing hearings are critically important, and I fully believe that this committee's vigilance has played a vital role in moving the ball forward. Don't go anywhere, though, because the country is not more secure yet. Thank you.

[The prepared statement of Ms. Brian follows:]



Testimony of
Danielle Brian, Executive Director
Project On Government Oversight
on
Nuclear Security:
Can DOE Meet Facility Security Requirements
Before the
House Subcommittee on National Security,
Emerging Threats and International Relations
April 27, 2004

Thank you for inviting me to testify today. The Project On Government Oversight (POGO) is heartened that this Committee has remained so active in overseeing the nuclear weapons complex and its ongoing security challenges. I must say, at your previous hearing I was relatively pessimistic that we would ever be successful in gaining any real security improvements from the Department of Energy (DOE). At the hearing, National Nuclear Security Administration (NNSA) Director Ambassador Linton Brooks announced the formation of yet two more commissions to review security around the complex: This announcement left us cold, as we had previously compiled a list of over 50 reports, testimonies, commissions, hearings and briefings issued between 1998 and 2002 concluding that security was inadequate at the DOE weapons complex. We didn't need any more. We still don't.

Since then, however, POGO has become more guardedly optimistic. We had the opportunity to meet with Secretary Spencer Abraham, Deputy Secretary Kyle McSlarrow and Security and Safety Performance Assurance Office Director Glenn Podonsky in January 2004. We began, in that meeting, ongoing communication with Secretary Abraham regarding our concerns and recommendations. We have reason to believe that he is taking these issues seriously. Our best evidence of that is the recent announcement that Los Alamos' Technical Area -18 (TA-18) is *finally* going to be de-inventoried of its Special Nuclear Materials (SNM).

666 11th Street, NW, Suite 500 • Washington, DC 20001-4542 • (202) 347-1122
Fax: (202) 347-1116 • E-mail: pogo@pogo.org • www.pogo.org
POGO is a 501(c)3 organization

Furthermore, two significant security policy directives have recently been issued. The new Design Basis Threat (DBT) issued last Spring requires that the sites be able to defend against a larger attacking force and a much larger truck bomb by 2006. The second directive is an April 5, 2004, requirement that all sites with weapons quantities of SNM increase their defensive posture to a "denial" strategy because of the Improvised Nuclear Device (IND) vulnerability. In other words, they must be able to prevent terrorists from even entering the facility because the terrorists could create a nuclear detonation within minutes. Both of these directives will require major changes in defensive strategies and upgraded infrastructure.

In the face of these requirements, the majority of the Category I sites containing weapons quantities of plutonium and highly-enriched uranium can no longer apply band-aids to their security problems. DOE simply no longer has the luxury of having SNM at sites that can't be adequately protected, or where the costs of protection are prohibitive.

This is a critical turning point in the direction of the nuclear weapons complex. The growing awareness by the DOE of the vulnerabilities posed by these sites is a hollow victory, however, without commensurate actions. The Department has to immediately begin to de-inventory certain sites, transferring the SNM to more secure sites; build underground storage facilities at Savannah River and Y-12; and blend down excess highly-enriched uranium and immobilize excess plutonium. These steps would make the nuclear materials far less attractive to terrorists.

In addition to highlighting the urgent need to move the SNM from TA-18, we raised several other priorities for the Secretary's consideration. This Winter, POGO began focusing on security at two additional NNSA sites: Lawrence Livermore National Laboratory just east of San Francisco and the Y-12 Plant in Oak Ridge, Tennessee. Both face serious physical security challenges – perhaps insurmountable challenges. We don't feel comfortable discussing publicly the specific concerns we have regarding Livermore security. However, we can say that the encroaching residential community surrounding Lawrence Livermore has made it nearly impossible to properly protect the weapons quantities of plutonium and highly-enriched uranium stored there. Clearly, they will not be able to comply with the new directives. If you haven't already, I would recommend the committee review "Systems Under Fire," a film produced by DOE's independent oversight office which demonstrates the lethality of the weapons that would be used by terrorists in attacking one of these facilities. In light of the facility's vulnerabilities, POGO recommends that all weapons quantities of plutonium and highly-enriched uranium should be de-inventoried from Livermore immediately and sent to the Device Assembly Facility (DAF) at the Nevada Test Site. Any research that requires weapons quantities of SNM can easily be accomplished by flying the Livermore scientists to the DAF, only a one-hour flight away. This move would dramatically increase security while saving about $30 million in annual security costs.

Some in DOE and the Congress have identified Y-12 as the most serious security concern in the complex. Y-12 stores hundreds of tons of highly-enriched uranium, and is a prime target for terrorists who would want to create an IND within minutes. Given the obsolete infrastructure currently housing the HEU, it should come as no surprise that the Y-12 guard force has been systematically cheating in order to pass security performance

tests. They simply cannot protect the materials in the six material access areas given the multiple targets, dilapidated infrastructure, and very short time lines for the terrorists to reach their target.

The current contractor operating Y-12, BWXT, inexplicably changed a plan to build a bermed facility covered by earth on three sides and its roof, similar to the DAF, and is now planning to build an above-ground facility. The change in design was approved based on the contractor's estimate that it would both increase security and save money. However, in a March 19, 2004, Inspector General report about Y-12, the IG concluded that the new design for the storage facility will actually *decrease* security and significantly *increase* costs. Project costs have skyrocketed, going from an estimated $144 million in 2001 to $253 million in 2004, while security features for the facility have been seriously degraded. Cost escalation is a classic foot-dragging maneuver that POGO has seen repeatedly throughout the nuclear weapons complex. All the security experts we have interviewed conclude that a bermed facility would be far more secure. Immediate funding for underground storage at Y-12, and the blending down of the over 100 tons of excess HEU, should be the top priorities of the NNSA budget. Again, this would lead to significant savings in annual security costs, because only one hardened facility would need to be protected, versus the current six aging buildings.

There have also recently been significant security problems at Sandia National Laboratory in Albuquerque, New Mexico. The only weapons quantities of SNM stored at Sandia are the highly-enriched uranium fuel plates for the SPR-III burst reactor. The reactor is rarely used. DOE had made plans in 2000 to move that reactor (machine and the fuel) to the Nevada Test Site. Although Lockheed Martin, the contractor running Sandia, agreed to the move, it never took place. This move would again drastically reduce security requirements and save about $30 million annually in security costs.

In addition, the Idaho facilities store tons of SNM – the second largest repository of highly-enriched uranium in the complex. These nuclear materials are left over from the Cold War and abandoned research projects – they have no current national defense mission. Tens of millions of tax dollars are spent securing these materials. These facilities should be de-inventoried of weapons quantities of SNM, again significantly increasing security while saving annual security costs.

DOE has publicly stated that the new Design Basis Threat (DBT) issued late last Spring is robust. However, POGO's sources have suggested that the DBT at most sites remains inadequate, far below the level of security recommended by the intelligence community, particularly at sites with IND vulnerabilities. As the General Accounting Office (GAO) pointed out in its report presented at your last hearing, the DBT was cost-driven: NNSA simply didn't want to spend the money to defend against a more robust and realistic threat. The GAO wrote, "DOE and NNSA officials from all levels told us that concern over resources played a large role in developing the 2003 DBT, with some officials calling the DBT the 'funding basis threat,' or the maximum threat the department could afford." This is not an acceptable method for determining security standards. The DBT should be reevaluated to bring it more in line with the realistic threat contained in the intelligence community's Postulated Threat, particularly for IND-vulnerable sites.

A final note regarding the TA-18 move: POGO is concerned that there are people in the complex who are still trying to sabotage this move. While POGO was heartened by the original announcement regarding the move, our hopes were dampened after meeting with the head of the nuclear weapons complex, Dr. Everet Beckner. Despite Secretary Abraham's intentions that all Category I Special Nuclear Materials should be out of TA-18 by 2005, Dr. Beckner informed us that NNSA only intends to move 50% of it. In a separate meeting, NNSA Administrator Linton Brooks told us that moving only part of the material would not improve security at all. (This is because enough material would remain behind to create an improvised nuclear device.) Dr. Beckner went on to inform us that the ballooning cost for this move – from $100 million to over $300 million – was in large part a result of the requirement to produce Authorization Basis documents to move the burst reactors from Los Alamos and to operate the reactors at the Nevada Test Site. He told us this paperwork requirement alone would cost $150 million. We checked with the person in the Los Alamos Area Office who is responsible for signing off on such documents: He estimated the cost to be between $1-2 million if done correctly, and as much as $6 million on the outside if it needs to be reworked. The reason I'm raising this is to illustrate how the bureaucracy knowingly provides completely baseless information to Headquarters as a way of protecting the status quo. I think it is essential that the Committee straighten out this confusion today during this hearing.

POGO is guardedly optimistic that Secretary Abraham and Deputy Secretary McSlarrow are sincerely concerned about the state of security at the nuclear weapons complex. However, these two officials have a limited time in office. The Office of Security and Safety Performance Assurance will be the entity left behind to oversee any improvements. Our concern is that the Office currently does not have either the necessary independence or power to see this difficult job through. POGO recommended in our 2001 report that this Office be moved outside the DOE in order to establish real institutional independence. At the very least, Congress needs to formalize its communications with this Office, as it has with the Inspector General.

Your ongoing hearings are critically important. I fully believe that this Committee's vigilance has played a vital roll in moving the ball forward. Don't go anywhere, though, because the country is not more secure yet.

Mr. SHAYS. Thank you very much.

We will start out by having the counsel ask some questions.

Mr. HALLORAN. Thank you.

To GAO, I would like to talk about the DBT development process a little bit. In your statement, in the report, you say one of the reasons it took almost 2 years to reiterate the DBT after September 11 was due to sharp debates within DOE and other Government organizations over the size and capabilities of future terrorist threats and the availability of resources to meet those threats. Could you talk some more about that? What other organizations, Government organizations, were involved? And what were the kind of parameters of the debate?

Mr. NOEL. Well, there were two debates that we are talking about in the report. One is the——

Mr. SHAYS. Bring the mic a little closer to you, please.

Mr. NOEL. There we go. My apologies.

Two debates. One is within the intelligence community that was developing the postulated threats. So when we reviewed the documents there and interviewed the participants, they all said that it was a lot of concern within the Department of Defense and the Department of Energy about how big a threat should we postulate and what can we afford. And when you look at the postulated threat there is in fact a range of adversaries that is postulated there.

Paralleling that, mirroring that, was a similar debate within the Department of Energy, and we looked at that a lot more closely because that was basically the charge of our report. And in that case, we interviewed officials at all the different sites, both DOE and contractor officials. We reviewed documents that were sent in by the contractors and site officials, and we talked to headquarters people. And here again we found a broad consensus that underlying the debate was, "Geez, can we really afford what we are talking about?"

Our concern is that the threat needs to be the threat, and then the issue of budget comes in as a secondary issue to say, "If we can't afford this, are we willing to accept a certain amount of risk?" And the Department's processes do allow for that.

Mr. HALLORAN. But is it your finding that the differential between the level of threat postulated by the intelligence community and the level of threat reflected in DBT was artificially discounted? Or are there other legitimate reasons to say that, in terms of our design basis threat and the facilities and the shape and the configuration of the complex, this is realistically what we need to be able to fend off?

Mr. NOEL. Well, we never found that, in fact, somebody said, "Let's make it smaller, specifically because of a dollar amount." What we did find, though, was that the postulated threat does say that each implementing agency—so that would be the Department of Energy, the Department of Defense—is allowed to use its own judgment in how it implements it.

The key here, though, is if you look at history, if you look at the past postulated threats back through time, and this process has been around quite a while, there was always a one-to-one relationship between the postulated threat and the design basis threat. In

this case, the Department decided to depart from that, and that's what we are taking issue with them on in our report as to why.

Mr. HALLORAN. All of you. In a matter of implementation of the DBT, you found a report that the time lines seem unrealistic. Could you tell us, explain more why that might be the case? And what are the disconnects that would make them not meet their target even at the end of fiscal 2006, I think, is the projection right now?

Ms. NAZZARO. Well, I think our concern overall is that it took them so long to develop. I mean, adversaries move very quickly, and they adapt very quickly. The 1999 DBT was to be for 5 years, and that was obsolete within 2 years because of the September 11th attacks. You know, then it takes us 2 years to develop a new DBT, and we are still years away from full implementation of that.

A faster process is definitely needed. We found the process that DOE used as far as consensus to formulate policy was very cumbersome and time-consuming.

Mr. HALLORAN. The implementation plans for the DBT, they'd come out in May 2003. Is that the right, the DBT? And the implementation plans were submitted or received in January of this year?

Mr. NOEL. Correct.

Mr. HALLORAN. And what can you tell us about those?

Mr. NOEL. Well, we reviewed the plans for the Office of Environmental Management and the National Nuclear Security Administration. I think—and Mr. Podonsky can talk to this—I think his office had some concerns about the quality of the material in the plans and some of the assumptions that were being made in the plans.

Beyond that, depending on what happens with the Secretary's special annex team, some of those plans may need to be revisited. And that's going to stretch out that time line even longer.

Mr. HALLORAN. Because of the improvised device kind of overlay they are putting out?

Mr. NOEL. That is what the special team is addressing, yes.

When we were at the sites and one of the things we asked fairly early on is, how long does it typically take you to come up with a new plan and implement it? And this would be not in the environment that we are in now. And they said 2 to 5 years. And that was a broad consensus across the complex. So that's why we said we are not optimistic that they could make the 2006 date.

Ms. BRIAN. I would just like to add to that, first of all, I mean, obviously, 2006 is ridiculous to be waiting that long when we had 2001. That's 5 years of actually implementing improvements.

But perhaps more realistically, what we are finding is if we are talking about the complex as it currently exists, it is simply impossible for these facilities to actually implement the requirements necessary between the DBT and this move toward a denial strategy, which we think is incredibly important. They can't do it. So something is going to have to significantly change.

Mr. HALLORAN. Let's stay with that, because in your testimony, you talked a great deal about the Y–12 storage facility and the IG report. What, in your view, drove the decision to change from the berm facility to a strictly above-ground one?

Ms. BRIAN. We have asked the contractor. They didn't have an answer. I can't speculate as to their motivation, but the conclusion is that what we are faced with now is a facility that is going to be more expensive and less secure. And I think the Congress has to step in and do something to stop this before they start actually moving earth in the wrong direction, because as we know, it's very hard to stop something once it's started.

Mr. HALLORAN. Does GAO have a view on that?

Mr. NOEL. Yes, just to add to what Ms. Brian is saying. The key here is that the DBT says any new facilities must meet all the requirements of the DBT. If it's an existing facility, certain requirements don't necessarily have to be met. So I think the IG's finding is very significant because it suggests, and we can't talk about all of this here, that this new facility isn't going to meet the standard that was just put out last May.

Mr. HALLORAN. OK. What's the significance of the TA–18 move?

Ms. BRIAN. It's the first step toward actually increasing security, an actual physical move to take materials out of a part of Los Alamos that is at the bottom of the canyon, which has been time and again proven to be an absolutely ridiculous place to be storing nuclear materials. And so by finally moving it, we are getting somewhere and actually making the space more secure.

Now, the problem is the people in charge of implementing it seem to have a different agenda from the Secretary. And I am hoping that this committee will be able to get a commitment from NNSA today that they actually intend to move all of it.

Mr. HALLORAN. Is it your sense, any of you can answer, that one of the kind of political dynamics here is that possession of special nuclear material is a budget credential, an institutional credential, it is something you want to keep and makes you less BRAC-able, as it were? What drives the need to keep the stuff when it's not being used?

Ms. BRIAN. There does seem to be sort of an emotional attachment by these facilities to these materials that I think they—honestly, I think it comes down to feeling less important if you don't have them.

Ms. NAZZARO. And one other issue that we have heard is that it does make it more difficult for the scientists. If you have the materials onsite, it is certainly easier for them to conduct their research.

Ms. BRIAN. Many of these facilities aren't actually using the materials for experiments at all, though.

Ms. NAZZARO. But our conclusion also, as far as a short-term action, was that DOE needs to consolidate some of these special nuclear materials.

Mr. HALLORAN. Could you go down your recommendations, and explain, flesh them out a little more for us, and give us a sense of priority in which you think would be the most urgent and which could be a longer-term goal?

Ms. NAZZARO. We certainly would like to see DOE address outstanding issues that we have raised with the current DBT, particularly as it relates to the improvised nuclear devices.

But I think, in a longer term, what you really need is a Department-wide implementation plan. This, you know, activity involves

more than NNSA. You need EM to be involved as well as Transportation Security Agency.

Mr. HALLORAN. And construction is a separate pot of money, too, right? And it has to be integrated?

Mr. NOEL. Correct.

Ms. NAZZARO. And that's what's missing right now. I mean, you have budget numbers in the current budget. But without a plan, I mean, this is only a down payment. We have no idea what its going to take to have full implementation of the DBT and what it's going to cost.

The other thing is we feel it is very important for them to inform you all, Congress, on what they are doing as far as the status and their strategies for implementation. I mean, this is going to take a lot of resources. It is going to be a costly venture.

Ms. BRIAN. Well, it's actually, obviously, we agree that it is going to be tremendously costly to implement the DBT given the complex as it exists. And that's one of the arguments for consolidating is that, in the long run, it would save money tremendously, because you could reduce the security requirements. Besides if you move the SNM, you don't have to have that level of security anymore.

Mr. HALLORAN. Your first recommendation talks about evaluating the cost effectiveness of existing SECON, security conditions. And what's your concern there?

Ms. NAZZARO. Well, last year, if you recall, DOE did take some immediate actions to respond to the September 11th attacks. And one of the primary methods was when the SECON level increased to put additional protective forces in place. That's a very costly exercise, and they did not have adequate resources to do that immediately, so there was a lot of overtime, which not only took a toll as far as financial constraints but also in the protective forces themselves. You know, they didn't get the training they needed. The fatigue set in, you know. There were a lot of downsides to that strategy.

Mr. HALLORAN. Well, that's the point that Ms. Brian raised in terms of the personnel force. Did you get a sense in terms of the DBT implementation plans that the first reaction was to throw bodies at the problem, and bodies that we may not have or we may wear out?

Ms. NAZZARO. Well, that was certainly one of their first strategies, and we do still think that protective force is a key element.

But we also suggested the increased use of technologies as alternatives to just the protective force that can help in this exercise?

Mr. NOEL. I think you need to recognize, though, that at least in the short run, and short run is probably during the timeframe that we are talking about here, putting more guards on these materials is really the only solution. And if you try to do it with too much overtime, you really lose the effectiveness of your guard force. For these people, standing there, watching the material is what they do pretty much all day long, and where you ensure that they are effective and that they are well trained is through the training exercises. If you have too much overtime, those exercises just don't occur.

Ms. BRIAN. And I would like to add to that point. I think Mr. Podonsky would be able to speak to a review he has done of the

guard force across the complex. But in our investigations, we found that, at Livermore, you have the guards who are working extraordinary hours, terrible morale problems. At Oak Ridge, you have guards who are working 70-hour workweeks for weeks on end. Most of them don't have time for training. So I think you have a tremendous problem with the guard force.

Mr. HALLORAN. Let's talk about the EM sites for a minute, if we could. It strikes me that as we succeed—and I think progress has been made, as you noted in your report. In kind of hardening the weapons facilities, the EM sites might become more attractive, and yet they don't seem to be a priority. It's a tough call. I mean, you don't want to spend all kinds of time and money hardening your places that you hope to make go away sooner or later. That's the more difficult balance overall, I think. What are the unique challenges posed by the EM sites at this point?

Mr. NOEL. The EM sites have the same kinds of materials that the NNSA sites do, so they have to be treated, in the end, in the same way.

But you are correct in observing that if you are trying to close something down, you don't want to hire a lot of guards that you are going to lay off 2 years later, especially since it takes a very long time to clear the personnel and to adequately train them.

So at some point in time, there is a tradeoff that is going to have to be made between cost and risk. And this is why we think it is really important, as we made in our last recommendation, for the Department to inform the Congress of these kinds of decisions so that the decision is made carefully and is well considered. And that's, basically, the sooner you can get these things closed, the sooner you can get that material moved, the better off you are going to be, the more secure those sites are going to be.

Ms. NAZZARO. And we are not saying that there will never be any risks. You know, risk is probably going to be a fact of life. But you need to have a measured risk, and you need to know what those risks are and what efforts we need to take to mitigate them to the best we can.

Mr. HALLORAN. My final question. Both testimonies talked about the need to kind of reassess or reevaluate the DBT. And I have to hope and assume you are not talking about launching another 2-year process to reiterate this thing. So could you be more specific in terms of what reevaluation might entail and what we could be doing in the meantime?

Ms. NAZZARO. Well, I think our primary point is one that Mr. Noel made just a few minutes ago, was that we are really concerned that DOE is not treating nuclear materials in the same way they are treating nuclear weapons. So that would be something that we would want immediate attention given to.

Also, the new DBT has identified additional threats in radioactive, chemical, and biological agents. In that area, there is no criteria as to their standards to defend to. In the area of chemical facilities they have said they are going to develop strategies to defend to industry standards. At this time there are no industry standards.

Mr. HALLORAN. So on what basis do they say that? I mean, how do they say that then? What do they think they are referring to?

Mr. NOEL. Well that's not really clear to us, and that's why we kind of put it back on them. This is their design basis threat. But I think there are standards. They have done a lot of research.

For example, I think, probably in the radiological area, they are furthest along. There is a lot of knowledge, about a lot of modeling, that is done at these sites of if there was an accidental release what the consequences would be. So you could use that information to basically better inform the standards that you are applying, rather than just simply say, "If anybody gets killed right on the site, we have a problem," because the problem is obviously much bigger than that.

Ms. BRIAN. We would also obviously—if DOE is willing to recognize that this DBT isn't adequate, which they haven't done yet, and they move up the implementation of the current DBT to being much sooner than 2006, with the recognition that the facilities are expected to have an either—a greater DBT in the near future. I think waiting until 2006 is one of the biggest problems we have, because we are not seeing a lot of activity. I think they are hoping that people will forget, administrations will change, and they can get back to the way things always were.

Mr. SHAYS. Thank you. I may ask the same question a different way, but it will help me understand it. We have production plants, test facilities, research labs, storage locations, and decommissioned sites. Have I left anything out? Production plants, testing facilities, research labs, storage locations, and decommissioned sites.

Ms. NAZZARO. And the Office of Secure Transportation.

Mr. SHAYS. Right. Which gets the plutonium and enriched uranium and the other materials of the weapons from one site to another site.

Mr. NOEL. As well as the weapons themselves.

Ms. NAZZARO. And transports the weapons from DOD to DOE.

Mr. SHAYS. It's a transportation issue—and that office—you all were only weighing in on the design basis threat. Correct? In your report?

Ms. NAZZARO. Yes.

Mr. SHAYS. So you were not looking at the logic—well, let me ask it this way. I happen to believe we have too many sites, and I believe we have too many sites for political reasons. And we have too much, too many structures on each site, and that's a cost issue. Do you disagree with either of my conclusions?

Ms. NAZZARO. I would say, no, we do not disagree as far as nuclear materials.

Now, we did not assess whether DOE has too many sites. But as far as nuclear materials, we feel that a first step is for DOE to consolidate some of those materials, that would help it in reducing the cost of the implementation.

Ms. BRIAN. We have taken the same position, that we are really just looking at the cost of having the materials in so many sites.

Mr. NOEL. And I think what Robin is saying is, you can consolidate materials within sites and then visit the broader issue of consolidating the sites themselves.

Mr. SHAYS. Have you done any research that shows that we need so many sites?

Mr. NOEL. No.

Ms. NAZZARO. No.

Mr. SHAYS. Is there any logic for why we need so many sites?

Ms. NAZZARO. You could look at history. I mean, that's what dictates where the current sites are. You know, is there a historic role in nuclear weapon production for the most part? But we have not done any current studies that would reassess post-cold war environment.

Mr. SHAYS. The concept of design basis threat, for my simple mind, I feel like a few people could get in a room, and in a week, they could do a fairly logical design basis threat. I mean, I want you to tell me why it would take months or years to figure out what is a logical design basis threat. Walk me through why it would take so long.

Ms. NAZZARO. I don't know that I could say it should take 2 years. And we have certainly said that 2 years was a long time to do this.

But we have to also realize that we had a different environment after September 11th. The United States had a different sense of a terrorist threat capability within the continental United States versus any places overseas.

Mr. SHAYS. Right.

Ms. NAZZARO. So this was a whole new paradigm, if you will.

Mr. SHAYS. That would speak to speeding up the process, not slowing it down. What's your point?

Ms. NAZZARO. Well, as far as that you are looking at a new paradigm, it's not just updating, but I mean, we had a significant change in factors, as to a terrorist threat. We can talk a little bit more specifically as far as numbers this afternoon.

Mr. SHAYS. We don't need to talk numbers right now. We need to just talk logically. I mean, we don't have to talk numbers to say that, in the past, we basically determined someone needed to get in and out, and now we have determined all they have to do is get in. And we are not telling anything that's top secret. The terrorists know that.

I mean, if they are willing to get on an airplane and blow themselves up in this missile that they have devised, we can instantly determine that a design basis threat that says what will it take to get them in and out is going to be a lot more difficult for the terrorists. And now, if all they have to do is get in, it's going to be a lot easier for the terrorists. I mean, that's pretty simple stuff. You wouldn't disagree with that?

Mr. NOEL. Let me see if I can give you a couple examples of things that came up as we were doing our work.

Mr. SHAYS. Sure.

Mr. NOEL. One was there seemed to be a fairly large debate among the intelligence community about September 11, and was this one group of 19 or 20 people, or four groups of 4 or 5 people? And that does sort of drive which way you are looking at the world in terms of how big the threat should be postulated at. In the case of——

Mr. SHAYS. Well——

Mr. NOEL. Now, I'm not going to defend either one.

Mr. SHAYS. No. But just walk me through that. I think I know what you mean, but I think I could come to some real different conclusions. So tell me what 19 means versus four groups of 5.

Mr. NOEL. Well, we really can't talk about that until this afternoon, I don't think, to be fair, because it gets to what number you would set for your postulated threat.

Mr. SHAYS. Let's not talk about what you would set. Just tell me what a large group versus what a number of collective small groups means. Walk me through that.

Ms. NAZZARO. Well, I think the issue was there was no agreement as to what we should be trying to defend against.

Mr. SHAYS. We won't even agree. I will just give you, if you have 20 people during an attack versus four groups of 5, tell me what the significant tradeoffs would be.

Mr. NOEL. Well, the significance was, were the four groups of five operating together, or were they independently just happening to arrive at the same place at the same time?

Mr. SHAYS. Or I could logically say to you that you could have 20 people getting in a plant, or you could have four different groups working together in groups of 5.

If we were in a Cabinet meeting with the President, you would have to take that phone that just went off and put it in a glass of water, if you don't know how to turn it off. That's basically what I figured I would do if I found myself in that circumstance.

No. I just want to understand that. You know, we don't need to talk secret stuff. I mean, is there any doubt in anyone's mind that these attacks weren't coordinated?

Mr. NOEL. Well, that was a matter of debate that drove a significant amount of the time involved here. And I will defer to the Department to let them explain that a little bit better.

Mr. SHAYS. It will be fascinating to understand that one.

Mr. NOEL. The other point I was going to make was when the Department did its own internal thing, what it would do is it would develop a design basis threat, send it out to all the sites and contractors. They would prepare written comments and concerns, and send them in. Those comments would get analyzed and put into a matrix, that would get circulated for review.

And as we point out in our report that went through about four or five iterations of this. So every time you did that, you had a lot of paper flowing back and forth, a lot of commenting and analysis of the comments. And it's just that whole process tends to be very laborious.

Our point being, that might be all right for some more general policy. But for this kind of a situation where the adversaries can move very quickly, maybe you need to relook at that and not go through that same process in the future.

Ms. BRIAN. Mr. Chairman, if I could add.

This is also relevant for your work in overseeing the commercial nuclear power plants, that the NRC, when they were looking at their design basis threat, were weighing in on this question of, "Well, we only need to protect, you know, a smaller group because this wasn't a coordinated effort of a larger group."

But something that I think might be missing in this conversation is what was raised earlier. After the postulated threat was estab-

lished, you then had the DOE separately making decisions about—and this is a big part of the time problem—well, are we going to accept the postulated threat at all?

And they sort of concluded, as GAO mentioned, for the first time, "Well, we've decided we are going to have DBT, which is actually less than the postulated threat."

Mr. SHAYS. Well, I will just react first to this whole debate of 19, 20 versus four groups of 5. It was a coordinated effort. No one doubts it. So, if anything, it speaks to the fact that they can take 19 people and use them in a coordinated way, and they can focus on one or two targets. So, I mean, it seems to me that that is a debate that should have lasted about 2 minutes. But we will get into the numbers later.

Well, I think I'm just going to state for the record that I have gotten nothing but cooperation from NNSA and Admiral Brooks, and I have appreciated the amount of work they have done to help us understand this issue. And so I want to put that on the record.

It just strikes me, as I went to three of these sites, that the task is quite difficult—they are very, very old sites—and that I would think that terrorists would design their attack based on what they think it would take to succeed. And so the irony is, then we would respond by saying what would it take to succeed, and then what do we have to do to prevent that from happening, not based on even historically what has been done, because I think that they demonstrated on September 11th that they can take small cells, have them work in a coordinated way against, at a precise period of time. And it just seems to me that they have—that the design basis for that would have to take that into consideration.

When we saw these sites and we looked at the design basis threat back last year, it was very clear to me that if they could meet the design basis threat, the design basis threat that they had devised was simply not adequate. It just simply wasn't adequate. And I could think in more than one way how they could overcome simply by two people inside instead of one or zero. I was astounded at seeing the encroachment of the public to these facilities. I was amazed at how many buildings I saw onsite and how easy it would be for someone onsite to have some protection and get very close to their target. And I mean, I could go on and on and on. And I'm not saying anything that anyone just looking at a picture wouldn't conclude.

You have answered to me why it would take so long, but what you basically have done is you have, Ms. Nazzaro, you have basically done in your report is you have basically said the design basis threat isn't adequate and you are basically saying it's vulnerable and you are basically saying that it's going to take too long to resolve.

Ms. NAZZARO. Correct.

Mr. SHAYS. Are you saying anything more than that?

Ms. NAZZARO. I think you have captured the three main points.

Mr. SHAYS. And because it's so straightforward, I don't believe I have much more to add. Is there anything else?

I think what we will do—excuse me. Ms. Brian, what I would do is invite any of the three of you to make any closing comment, and then we will get on to our next panel.

Ms. NAZZARO. I think I would just like to reiterate our recommendations to try to move——

Mr. SHAYS. Why don't you run through them?

Ms. NAZZARO. I will summarize, but what we are trying to do is to expedite full compliance of the DBT. And first is to address the outstanding issues, particularly as they relate to the improvised nuclear devices; second, to develop that Department-wide implementation plan; and third, to inform Congress of that implementation status and any facility vulnerabilities that may affect either the surrounding communities or the Nation at large.

Ms. BRIAN. I would just like to affirm what the GAO has said. I think those are the most important steps. And I think that perhaps today, by the committee getting to the bottom of the first step toward that, which is the TA–18 move and establishing whether this place is actually getting deinventoried or not will start the ball rolling finally.

Mr. SHAYS. Very good. Thank you for your very important work.

And we will now get on to the next panel. That would be Linton Brooks, Administrator, National Nuclear Security Administration, Department of Energy; Glenn Podonsky, Director, Office of Security and Safety Performance Assurance, Department of Energy.

And I will invite you to come forward and remain standing, and I will swear you in.

[Witnesses sworn.]

Mr. SHAYS. I should have asked, is there anyone else who may join you in testifying? If there is, I probably should ask them to stand.

Mr. PODONSKY. Mr. Chairman, I would like to ask the Director of Security and the Director of Independent Oversight to stand.

Mr. SHAYS. If they will just stand, I will just swear them in. You two gentlemen can sit down. Is there anyone else, Ambassador, you would ask to be joining you?

Mr. BROOKS. I think I am flying solo.

Mr. SHAYS. You may not be asked to speak. And if you are, we will make sure your name is on the record.

[Witnesses sworn.]

Mr. SHAYS. Let me just read a statement, but first, let me again thank you Ambassador Brooks and you Mr. Podonsky, you have both been extraordinarily helpful to this committee. You have not been reluctant to tell us whatever we need to know. We couldn't have asked for greater cooperation.

We may have some disagreements. We don't face some of the challenges you face, but you are—we appreciate the good work you do, and we will look forward to getting into details in our closed hearing but also to talk about some important general concepts.

I would like to just make this statement—in response to our invitation letter of March 23rd, DOE informed us just yesterday that no witness was available to testify specifically on DBT implementation and decommissioned environmental management sites.

Those facilities possess unique vulnerabilities and possess difficult questions about the extent, pace, and cost of security enhancements. Unable to address those issues today, we will convene a separate hearing on DBT implementation at DOE environmental management sites. We have the Department's commitment to

make a high level witness available at that time. We would have liked to have done it today, but it just means it will get a special focus, which is I guess, what they wanted.

So, Mr. Brooks, welcome. What we do is we do a 5-minute statement, but we roll over 5 minutes, so you have up to 10. We hope you will stop somewhere between 5 and 10.

And may I also say that I understand you have some personal challenges at home, and we do appreciate that you take this job so seriously that you would meet your commitment here as well. And we thank you for that.

STATEMENTS OF LINTON F. BROOKS, ADMINISTRATOR, NATIONAL NUCLEAR SECURITY ADMINISTRATION, DEPARTMENT OF ENERGY; AND GLENN S. PODONSKY, DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE, DEPARTMENT OF ENERGY

Mr. BROOKS. Thank you, Mr. Chairman.

Thank you, Mr. Chairman. Before I get into my prepared remarks, I would like to make a couple of points about the panel you have just heard. And we can go into these at whatever length you want.

From my perspective, while I'm sure there was somebody who was worried about the cost of the design basis threat, I don't believe it's correct that cost was a driver in the decisions the Secretary made. I don't believe it's correct that the challenges at Lawrence Livermore will preclude adequate security or meeting of the design basis threat. I don't believe it's correct that the Inspector General found systematic cheating at Y–12. The Inspector General specifically said he could not document the allegations he had heard.

Nonetheless, both Mr. Podonsky and I think that any compromised performance testing is unacceptable, and whatever was true in the past, there won't be any in the future.

I don't believe it is correct that the HEU materials facility at Y–12 is an inferior design to the so-called berm design. In fact, it is a superior design. And I don't believe it's correct that only 50 percent of the material from TA–18 will be moved to Nevada. It's our intention to move all of that material. And I appreciate the committee's indulgence, and I will be happy to expand on those. And with your permission now, I appreciate the opportunity to appear before you. I have submitted a prepared statement which I would like to summarize.

Tightening the security that began with the establishment of NNSA in the year 2000 and accelerated after September 11th has resulted, in my view, in a strong, effective security posture at all nuclear weapons research and production facilities. Today, no nuclear weapons, no special nuclear material, and no classified materials are at risk within the nuclear weapons complex.

That does not mean that we don't have a great deal of work to do yet. Secretary Abraham has made it clear that we can't fulfill our mission unless we can guarantee security. That priority is reflected in our 2005 budget request as well as in the reprogramming request to be submitted this week. Our safeguards and security budget has grown from $400 million in fiscal year 2001 to $707

million in the current budget request. That's a 75 percent increase. The number of protective force officers guarding our facilities has increased from 2,100 to over 2,400 during the same timeframe.

Overall, security performance as measured by independent review has continued to improve. In the past year, no force-on-force performance testing by the Office of Security and Safety Performance Assurance has found security forces unable to protect special nuclear material on their site.

Now, while I am pleased with the progress we have made, our long-term security has to be based on more than guns, gates, and guards. Therefore, Mr. Podonsky and I will jointly commission an examination of how we can harness the power of technology to improve security.

We're already doing a great deal of that, which I will be happy to talk about in the question period. But we will explicitly look at what else might be done, and we will do so in time to affect the 2007 budget.

We will also look at accelerating the fielding of the technology we already have in hand. We believe that we must reduce our reliance on an old and aging physical security system and replace it with state-of-the-art technology.

But while we prepare for the future, we have to deal with today's threats. All NNSA sites have completed and I have approved plans to meet the design basis threat by the end of fiscal year 2006. We'll use formal vulnerability analysis to validate the security upgrades that I've improved. These efforts are under way.

Because we have not fully formulated our plans at the time of submitting the fiscal year 2004 budget, we're also submitting a $55 million reprogramming request this week to keep our design basis threat implementation on track. That will bring our budget for this year to $638 million. We've asked for another $90 million specifically for design basis threat in the 2005 budget request.

Mr. SHAYS. Let me just interrupt you. Are you saying you're asking for a supplemental——

Mr. BROOKS. I'm asking for reprogramming in this fiscal year.

Mr. SHAYS. Within your budget or within DOE?

Mr. BROOKS. Within mine.

Our most significant site, which is the Pantex site, and the Office of Secure Transportation, which moves both material and weapons, are already prepared to meet the design basis threat; and I'm confident that all sites will be in compliance by the end of fiscal 2006.

Let me now briefly turn to the GAO report issued today.

GAO spoke of the effectiveness of elevated security conditions. As the report states, we raised from SECON level 4, which we used to think of as normal, to SECON level 2 within hours of the attacks on September 11. The idea of these measures, which are tailored to each site, is to put up the best available defense against a broad spectrum of threats. We've validated these measures somewhat through tabletop analysis and through oversight, and we have modified the procedures over the last 2½ years to improve the effectiveness of SECON levels. Today, as a routine basis, we maintain SECON 3.

Seven times we've elevated our security condition, in each case in response to the Department of Homeland Security elevating the

overall threat level. As GAO quite correctly states, a heightened state of readiness impacts training, effectiveness, and the protective force. It also costs money. We estimate it costs about $560,000 a day for every day that we are in a heightened alert status. So we need to improve our ability to guard our facilities without throwing people at them, and we need to reduce the amount of overtime security force personnel are required to work.

We're aggressively hiring more security forces. Last year, the Congress approved a recommendation by the Secretary to give us additional flexibility in conducting background investigations to speed up the clearance of our new hires. We are, as I said earlier, trying to accelerate the use of technology—and we can talk about some of this in the question period—as a way to increase the effectiveness of security forces.

Secondary in the GAO report is improvised nuclear devices, and there's very little I'd like to say in the open session on this. However, we disagree with the GAO conclusion that an improvised nuclear device should be thought of as the equivalent of a nuclear weapon. Our reasoning was based on analysis of physics and weapons design, and we believe that nuclear weapons deserve the highest priority protection. That's because to detonate and improvise a nuclear device an adversary has to make that device into a condition where a nuclear weapon already is, and we believe that is a greater challenge and therefore we believe that the highest security should be reserved for nuclear weapons.

I'd like any further discussion of this, for fairly obvious reasons, to be in closed session.

I know that the security of Y–12 is of particular concern to this committee. It's certainly got some of the most difficult security problems anywhere in the complex. It's old. Facilities were built-in the early days of the cold war with no thought of the kind of threat we have now.

I am, however, still convinced that Y–12 will meet the deadline for implementation. Much of the funding for security upgrades that I referred to earlier has been used for improvements at Y–12, and much of the—about half of the $55 million reprogramming—will be in Y–12 and about $25 million of the design basis threat money in the 2005 budget will be for Y–12.

Now that level has led a number of people, including I believe you, Mr. Chairman, to question the long-term viability of Y–12 as a site for this mission. Secretary Abraham has committed to another committee of the House of Representatives to conduct a zero-based review of the entire weapons complex, based on a revised stockpile plan which is in the final stages of approval and a look at the design basis threat. He is committed, and we are committed to looking at all options.

It's clear, however, that if one of those options led you to conclude that you had to move Y–12 it would be a lengthy and expensive endeavor. It would take at least a decade, cost probably billions of dollars, and during that time Y–12 security would have to meet the same standard we are trying to achieve by the end of fiscal year 2006. So whatever the long-term merits, I do not believe moving Y–12 or any other site is a solution to our near-term problems.

I do, however, agree with the testimony you've heard that consolidating and securing special nuclear material is an important part of our security strategy. We are well under way in our plan to begin moving material from TA–18 to Nevada this calendar year. We are also looking at other material consolidation candidates.

I believe consolidation, as referred to in the last panel, is important within sites. For that reason, the highly enriched uranium material facility in Y–12 is particularly important because it will allow us to consolidate within the site and reduce the defended footprint.

At the same time, sir, consolidation is not a panacea. We have to have materials at some locations to carry out our mission.

For example, the subcommittee has heard suggestions to eliminate special nuclear material at Lawrence Livermore. In our judgment that would preclude our carrying out our stockpile stewardship assessments; and that's because, while we can move the material someplace else, we can't move the research capabilities and processes that exist at Livermore.

In conclusion, sir, we are fully committed—the Secretary is committed and I am committed to maintaining security at our facilities. Implementing the new design basis threat is a major part of that effort, and I am confident that we will continue to ensure the security of the complex.

I thank you for your attention, sir; and I'm looking forward to your questions after you've heard from Mr. Podonsky.

Mr. SHAYS. Thank you, Ambassador.

[The prepared statement of Mr. Brooks follows:]

Testimony of Linton F. Brooks, Under Secretary for Nuclear Security and Administrator, National Nuclear Security Administration
Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations
Hearing on Nuclear Security: Can DOE Meet Physical Facility Security Requirements
Tuesday, April 27, 2004

INTRODUCTION

Mister Chairman, members of the Subcommittee. Thank you for this opportunity to address security at the National Nuclear Security Administration' s nuclear weapons research and production facilities as well as the issues raised in the General Accounting Office's report on implementation of the May 2003 Design Basis Threat.

The tightening of security that began with the establishment of NNSA in 2000 and accelerated in the wake of the September 11, 2001, terrorist attacks, has resulted in a strong, effective security posture at all nuclear weapons research and production facilities. Today no nuclear weapons, Special Nuclear Material, or classified materials are at risk anywhere within the nuclear weapons complex. We are hard at work to sustain that improvement in the security of the complex over the long term.

Secretary Abraham has made it clear we cannot fulfill our national security mission unless we can guarantee security at our facilities. In recognizing security as essential to our mission, he has directed spending on security take priority over other program spending until we can guarantee that security. This priority is reflected in our Fiscal Year 2005 budget request with its significant growth in security spending as well as in a reprogramming request to be submitted this week. Our safeguards and security budget

has grown from $411 million in Fiscal Year 2001 to $582 million in Fiscal Year 2004 and we have asked for over $707 million next year. That's a 75% increase since 2002. About half of this funding is spent on the protective forces that provide front-line security at NNSA facilities. The number of protective force officers guarding our facilities has increased from 2100 to over 2400 during that same timeframe. Overall security performance as measured by independent reviews has also continued to improve. In the past year, no force-on-force performance testing by the Office of Security and Safety Performance Assurance has found security forces unable to protect the assigned assets on their site.

While I am pleased with the progress we have made, our long-term security must be based on more than guns, gates, and guards. Over the long term, we are committed to harnessing the power of technology to improve security. To leverage this power, Secretary Abraham has committed the Department to two initiatives. The first is commencement of a study of DOE requirements and the technologies available today to meet those requirements. We plan for this study to be completed in time to effect changes in the Fiscal Year 2007 Budget submission. The second initiative will re-establish a robust, active research and development program focused on accelerating the availability of new security related technology to the field.

These complementary efforts are designed to reduce our reliance on costly, aging, maintenance- and labor-intensive physical security systems and replace them with state-of-the-art systems designed to put the assets we protect beyond the reach of even the

most capable adversary. In the Twenty-First Century, America's technological prowess can provide invisible gates, omniscient over-watch, and lethal, accurate response capable of deterring or defeating any adversary. We will move toward that future.

But while we prepare for the future, we must deal with today's threats. All NNSA sites have completed, and I have approved, plans to meet the Design Basis Threat by the end of Fiscal Year 2006. We are working closely with our colleagues in the rest of the Department of Energy to ensure those plans meet the rigorous test of the DBT. To that end, we fully agree with the comments from the Office of Security and Safety Performance Assurance on the need for vulnerability analyses to validate planned security upgrades as well as the need for detailed schedules for achieving implementation milestones. These efforts are now well underway at each site and a detailed schedule for validation and testing is taking shape.

We have a number of initiatives and actions under way that demonstrate our commitment to meeting the DBT by the end of Fiscal Year 2006. Since our DBT requirements were not fully evaluated before the formulation of the Fiscal Year 2004 budget, we analyzed this year's budget to identify $55.4 million for reprogramming to keep DBT implementation requirements on track. That would bring our total budget for this fiscal year to $638 million. We have included another $89.9 million, in addition to the base, for these requirements in our Fiscal Year 2005 budget request and anticipate providing the necessary funding required in Fiscal Year 2006 and beyond.

Our Nuclear Safeguards and Security Programs office is leading a team of security and budget specialists to each site to make sure their budgeting processes captures all security requirements and ensure headquarters and sites are in agreement on priorities and the way forward. A second team of experts has just completed visits to every site to review locks and keys procedures, collect best practices, and make recommendations for improvement. I have been briefed on the results of that review and plan to issue NNSA policy guidance to upgrade existing locks and keys programs. In the long term, I intend to pursue an initiative that will move us toward a "keyless" security environment within the next five to ten years.

We have also used experts from outside the Administration to help improve the effectiveness of security. I have recently received a report from Admiral Hank Chiles on the health and future of the NNSA' Federal security workforce. My staff is in the process of developing an action plan to address the study's findings and recommendations. In very short order, I expect to receive reports from Admiral Rich Mies on the overall effectiveness of NNSA security operations.

These reports will be a central focus of the NNSA Safeguards and Security Summit I will hold in June with the top Federal, laboratory, and plant managers together with their senior security staffs. My plan is to seek their input on how best to implement the recommendations in these reports to enhance security effectiveness and better manage the security career field. This will be the first such summit NNSA has ever held.

Our corporate partners have also reaffirmed their commitment to security. For example, the University of California has established a security oversight board for Lawrence Livermore and Los Alamos National Laboratories. Lockheed Martin, prime management and operations contractor at Sandia, has established a Security Subcommittee of their Board of Directors to ensure appropriate continuing independent focus on Sandia National Laboratories. We have new security chiefs in place at several of our laboratories and plants, and we are beginning to reap the fruit of these changes.

The Administration's efforts to meet the security challenges raised by the 9/11 attacks have been well documented in both the GAO report issued today and in previous testimony before this subcommittee. Accordingly, I will not recount those efforts now except to establish them as the foundation for all subsequent and future measures. The process of enhancing security at NNSA facilities has been an iterative one and each step builds on the previous one and impacts the next in terms of the manpower and resources to proceed.

GAO

The GAO report raised the issue of the effectiveness of elevated Security Conditions or SECONs at NNSA sites. As the report states the SECON at NNSA sites was raised from SECON level "4", or normal, to SECON 2 within hours of the attacks in New York and Virginia. These site-specific SECON measures, generally equivalent to prudent measures taken to protect life and property by American security forces worldwide, are designed to put up the best available defense against a broad spectrum of threats and deter attack by

raising the profile of security forces. Each site's SECON Implementation Plan is reviewed and approved by the NNSA site managers.

The effectiveness of SECON measures is validated through "table top " analysis, limited scope performance testing, alarm response drills and oversight by Federal site staff. Those facilities at greatest risk or with the highest potential of catastrophic consequences continually assess the effectiveness of SECON measures for critical areas and the effectiveness of the site protective force to meet mission assignments. Over the last two and one half years, sites have modified their security measures to reflect changes in threat levels in response to guidance from Headquarters. As I stated earlier, testing on measures to meet the new DBT are underway.

Today, our sites maintain SECON 3 plus additional security measures as a normal state of readiness. During seven periods since 9/11, sites have been directed to elevate SECON levels consistent with Department of Homeland Security setting Homeland Security Condition Orange. As the GAO report indicates, a heightened state of readiness does impact training, effectiveness, and the operation s tempo of the protective force. Additionally, we estimate the cost of SECON 2 averages about $560 thousand per day NNSA wide—most of that in protective force overtime costs.

We also recognize the need to reduce the amount of overtime security force personnel are required to work. We are aggressively hiring required additional security personnel to alleviate this problem in the short term. At our request, the Congress last year provided

us additional flexibility on conducting the necessary background investigations to allow these new officers to be effective. Additionally, the Secretary issued guidance in September of last year requiring the application of technology solutions to security challenges to the extent possible to reduce reliance on protective forces. In cooperation with the Office of Security and Safety Performance Assurance, we have begun a major initiative to employ available new technologies to enhance security and reduce costs. The NNSA Safeguards and Security Engineering Team—a multi-discipline, multi-site group - is an integral part of this process committed to promoting excellence in design, implementation, operations, and integrity of security systems at NNSA sites.

Improvised Nuclear Devices

As indicated by the GAO report, those scenarios where there is a threat of detonation of an Improvised Nuclear Device, or IND, were not necessarily considered the highest category of risk. The reasoning behind our assignment of risk categories was based on the analyses of physics, weapons design, use control, and security professionals working on the DBT and follow-on guidance. Under the graded protection concepts used within the Department, the Office of Security and Safety Performance Assurance, with substantial support from my staff, concluded a complete, assembled, and certified explosive device or weapon deserves the highest protection as it is already configured with Special Nuclear Material and High Explosives in close and correct proximity. In contrast, an adversary's ability to detonate an IND is primarily a Special Nuclear Material control issue. The adversary must achieve the conditions already extant in a weapon by gaining access to materials stored in substantial fixed facilities with protection in depth

and protective forces on site. For this reason, NNSA concurs with the rationale for such a determination.

Any further discussion of this issue should be conducted in closed session.

DBT Implementation

As I stated earlier, I have received and approved DBT Implementation Plans from the NNSA sites and we are tracking progress through quarterly reporting. The Fiscal Year 2005 budget submission includes specific DBT funding and I expect the Fiscal Year 2006 budget will be strongly influenced by DBT requirements.With planned FY 2004 reprogramming, Pantex and the Office of Secure Transportation will be prepared to meet the new DBT in 2004.. I can assure the members of the sub-committee all sites will be in compliance with the DBT by the end of Fiscal Year 2006 using a combination of fixed improvements and compensatory measures.

In fact, many of the basic improvements to physical security required for DBT implementation have been accomplished or are well under way. Some facilities have already been hardened. Critical material has been consolidated and the frequency of patrols around retained materials and critical facilities has been increased. Vehicle parking and movement has been controlled to increase the standoff distances around facilities for protection from vehicle bombs. Vehicle searches, including canine searches for bomb detection, have been stepped up. Temporary vehicle barrier systems have been put in place and construction of permanent barrier systems has begun.

We have not just increased the number of protective force personnel; we are continually improving their capabilities to defend against determined attack. Security positions are being hardened against blast and heavy weapons. To deny an adversary cover, lighting has been improved and fields of fire cleared around perimeters and critical facilities. Protective forces are being equipped with thermal imaging and night vision devices to further enhance their ability to detect and engage any adversary. And, when and if they must engage, protective forces will be using upgraded weapons and munitions with increased range, accuracy, and lethality.

Y-12

I know that security at the Y-12 facilities at Oak Ridge, Tennessee, is of particular concern to this Subcommittee. These facilities do represent some of the most difficult security problems we face in some parts of the complex—aging, outdated facilities built in the early days of the Cold War-- or earlier- when no threat of the current nature was envisioned. The long list of compensatory measures, capital improvements, and security upgrades identified by Site Office management to ensure Y-12 can meet the DBT clearly indicates the magnitude of the effort.

I am, nonetheless, convinced Y-12 will meet the deadline for implementation. Much of the funding for security upgrades since 9/11 has been used for interim improvements at Y-12. In addition to the $82 million appropriated for Y-12 this year, $7.5 million in headquarters funding was allocated to Y-12 and nearly half the $55.4 million in our

reprogramming request is earmarked for Y-12. The overall NNSA Fiscal Year 2005 security budget contains a request for $89.9 million for DBT implementation requirements and approximately $25 million of that is earmarked for Y-12. An appropriate percentage of the Fiscal Year 2006 funding will also go to Y-12.

This level of effort and funding has led some to question the long-term viability of Y-12 as an appropriate site for this mission. Secretary Abraham has committed to conducting a review of the entire weapons complex, based on the anticipated revised stockpile plan now under preparation and the new Design Basis Threat. We are committed to a complete review looking at all options. It is clear, however, that moving Y-12 would be a lengthy, expensive endeavor that would impact the mission for at least a decade and would costs billions of dollars. During that time period, security at Y-12 would have to meet the same standard we are striving to achieve by the end of Fiscal Year 2006. For this reason, I do not believe moving Y-12 is a solution to our near term problems.

We are doing more at Y-12 than just spending money. All our management and expertise are appropriately focused on Y-12's security issues. I have asked the Chief of Defense Nuclear Security to focus the majority of his time and attention to ensuring Y-12 stays on schedule to meet the implementation deadline.

Materials Consolidation

Consolidating and securing special nuclear materials is a major part of our overall security strategy. We are already well underway on our plan to begin to move Special

Nuclear Material from TA-18 to the Device Assembly Facility in Nevada as early as this calendar year and well ahead of the schedule. It has been a lengthy process and it's not over yet, but we have learned many lessons. To capitalize on those lessons, and under the banner of the Secretary's Management Challenges, my staff -- teaming with colleagues in Acting Undersecretary Garman's organization- is working to identify and prioritize other material consolidation candidates and develop a road map for streamlining the process for future consolidation efforts. Consolidation is important within sites as well as between sites. For example, the Highly Enriched Uranium Material Facility (HEUMF) at Y-12 will allow us to consolidate materials within the site and reduce the defended footprint.

At the same time, it is important to recognize that consolidation is not a panacea. Material must be at some locations in order to carry out our mission. Thus, for example, although the Subcommittee has heard suggestions to eliminate special nuclear material at the Lawrence Livermore National Laboratory, our judgment is that such a step would preclude our carrying out important Stockpile Stewardship assessments.

Conclusion

We at NNSA are fully committed to maintaining the security of the national treasures we guard. Implementing the new DBT is a big part of that job. With your support, we can continue our excellent track record, fix our problems, and ensure the long-term security of the nuclear weapons complex.

Thank you for your attention. I look forward to your questions.

ADDITIONAL COMMENTS BY LINTON BROOKS
ADMINISTRATOR, NATIONAL NUCLEAR SECURITY ADMINISTRATION
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives
April 27, 2004

Mr. Chairman, before I get into my prepared remarks, I'd like to correct the record on some points raised by the previous panels.

- It is not correct that the Design Basis Threat was limited for cost reasons. The final recommendations to the Secretary did not discuss costs, only requirements.

- It is not correct that the physical security challenge at the Lawrence Livermore National Laboratory resulting from residential encroachment makes adequate protection nearly impossible. In fact, the Office of Oversight and Performance Assurance tested the protective force capabilities at LLNL in February 2004 in a series of performance tests and found their capabilities satisfactory. We have no reason to believe that LLNL will not be able to comply with the revised DBT policy; they are currently on a path to meet his FY 2006 implementation schedule.

- It is not correct that the IG found "systematic cheating" on the part of the protective force at Y-12. Although there were allegations, the Inspector General "...could not find documentary evidence to support or refute the testimonial evidence" on this matter. In any event, such protective force improprieties are totally unacceptable and we have taken steps to ensure they do not occur in the future.

- It is not correct that the proposed new HEUMF facility at Y-12 will decrease security. The new design is superior to the early berm design because it provides "defense in depth" through a layered security approach. The original design provided substantially less security. To develop a berm design with comparable security features as the selected design would result in a facility which would be much more expensive.

- It is not correct that only 50 percent of the Category I/II material at TA-18 will be moved to the Device Assembly Facility in Nevada. All the material will be moved.

Mr. Chairman, I appreciate the Committee's indulgence, and therefore I would like to ask that the Committee allow me to provide a more detailed response for the record. With that Mr. Chairman, let me get on with my prepared statement.

Mr. SHAYS. What I'm going to do is I'm going to have Mr. Podonsky speak, but just to tell you what my question will be, I will want you to run down each of the points that you agree and disagree with GAO on.

Mr. BROOKS. Sure. Now, sir?

Mr. SHAYS. No, just after he's done. I'm just giving you a warning of what I want to ask.

Mr. Podonsky.

Mr. PODONSKY. Thank you, Mr. Chairman; and thank you for inviting me to testify today.

You requested that we address the issues as they relate to the GAO report dealing with DOE's implementation of its revised design basis threat. I have addressed those issues in detail in my written statement which I request be submitted for the record.

I would first like to commend the GAO for their thorough and professional job in preparing their report. We agree that the issues they raised are legitimate and valid and must be addressed. As acknowledged in the report, we had previously identified and we're dealing with some of those issues. We conclude, as I believe that GAO has also concluded, that while the issues raised in the report are important many of them describe past events and of more importance are DOE's current actions to improve protection programs and to implement the revised DBT. Therefore, I will only briefly mention the issues raised in the GAO report and will devote the bulk of my allotted time in discussing what we are doing to advance security and fully implement our revised DBT.

The issues raised in the GAO report essentially deal with the time it took to develop and issue the revised DBT and the differences to the threats described in the postulated threat and the DBT. Additionally, two issues deal with the effects of the manpower and intensive measures implemented on and after September 11, 2001, and the fact that effectiveness of these measures were not evaluated using our formal vulnerability assessment methodology. The final issues involve DOE's need to provide additional implementation guidance, implementation plans, and supporting budgets associated with revised DBT.

We accept these issues as valid. The Department's senior leadership is committed to fully meeting the agency's security responsibilities, including the timely implementation of the revised DBT. That commitment is reflected in Secretary Abraham's recent creation of my organization, the Office of Security and Safety Performance Assurance.

While the Secretary holds line managers accountable for effectively implementing security programs, he recognizes that the Department's effort to improve protection programs could be accelerated and more effective if relationships and interactions between headquarter's elements and the fields were improved.

His direction to me when he created the office, resulted in four major priorities: improve communications and cooperation between my two organizations and the field, improve the quality and security policy and policy guidance, evaluate and develop security-related technologies and make them quickly available to the field, and overall security training to ensure that national level training resources are responsive to the needs of field organizations. I believe

improvements in these four areas are key not only to our current efforts to upgrade security and fully implement the revised DBT but also to the future vitality of our protection programs.

We are improving the communication between my two offices and other headquarter's offices and security professionals in the field. We're working hard to ensure that organizational relationships are mutually beneficial and supportive of protection program needs. We have removed some institutional barriers that have hampered communications and have been successful in opening additional lines of dialog between my office and other organizations and agencies.

Our security policies and implementation guidance are the foundation of our protection programs. We believe that security policies should be practical, based on real needs and unambiguous.

Some of our policies have fallen short of this mark. A major contributing factor to past difficulties in resolving policy issues was a prohibition against policy developers communicating directly with field sites. The Deputy Secretary recently directed a change to this ill-conceived practice, and we have established necessary dialogs to facilitate policy development and revision. Our policy staff is currently at work reformulating and improving many of our security policies.

The Secretary sees our ability to implement new security technologies as a crucial element in our effort to fully implement the revised DBT. We are convinced that improved technologies will be a long-term key in our efforts to improve the effectiveness and efficiency of our protection programs. Whenever possible we have to move away from the very costly and often inefficient manpower-intensive responses to security concerns. The tendency to add more guards must change. The introduction of new technologies, such as active and passive barrier systems, can act as force multipliers that reduce our dependence on manpower.

The Department has the scientific and technology resources to address our technology needs. We are beginning to focus and improve our internal efforts in this area in cooperation with the NNSA and provide the field with technological options that can be used to reduce manpower and improve protection systems' effectiveness.

Security training is our final focus area. Through our National Training Center, we establish security training standards and provide safeguard security related professionals training for the Department. We intend to increase the efficiency and effectiveness of those efforts by ensuring that the training resources are more responsive to the specific needs of DOE and NNSA field organization.

We are focusing considerable effort in these four areas; and we firmly believe that Secretary's instincts will prove to be correct, that these initiatives will have a profound effect on our efforts to strengthen our protection programs. The Department's leadership has declared and demonstrated its willingness and determination to take the actions necessary to improve our security performance and to fully implement the revised DBT on schedule. We fully intend to pursue our efforts until we have achieved a Department-wide level of performance that meets our expectations, the expectations of Congress and of the American people.

I'd like to close by saying in my 20 years of working as the Department's overseer and now as the Department's overseer and policy promulgator, I have never seen an administration that was so committed to improving security as this administration under Secretary Abraham, Deputy Secretary Kyle McSlarrow and Administrator Ambassador Brooks.

Mr. SHAYS. Thank you.

[The prepared statement of Mr. Podonsky follows:]

STATEMENT OF

GLENN S. PODONSKY

DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE

DEPARTMENT OF ENERGY

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

April 27, 2004

Unclassified Congressional Testimony
Subcommittee on National Security, Emerging Threats, and International Relations
House Committee on Government Reform
April 27, 2004

Introductory Remarks

Mr. Chairman and honorable members of the subcommittee, I want to thank you for inviting me to testify today regarding the Department of Energy's processes for developing, evaluating, and implementing its Design Basis Threat, which it uses as a benchmark to develop and evaluate protection systems throughout the Department. We agree with the Subcommittee's assessment that the current threat environment facing the Department – and indeed facing the entire nation – represents a considerable potential risk to our facilities, assets, and personnel. Everyone in the Department having security responsibilities – from the Secretary to our armed protective forces and our individual employees – is aware that we live in dangerous times and that we have custody of particularly sensitive information, materials, and facilities that must be protected from a range of potential adversaries. We do not take our protection responsibilities lightly. The Secretary, Deputy Secretary, and NNSA Administrator are committed to meeting our protection challenges and have provided the impetus for numerous improvements in our protection programs, some of which I will discuss in this testimony.

The Subcommittee has asked that we specifically address several issues as they relate to the General Accounting Office's report: *Nuclear Security: DOE Needs To Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*. In responding to the Subcommittee's request, I will start by addressing the specific issues highlighted in the GAO report, and will then describe the specific role of my organization, the Office of Security and Safety Performance Assurance, in the Department's implementation process for the revised Design Basis Threat. I will then describe what we consider to be a directly related and more important issue: the several key initiatives now underway that will significantly

aid our efforts to improve the performance of our protection programs and facilitate our efforts to fully implement the requirements of the revised Design Basis Threat on schedule. Let me begin then with the specific issues raised in the GAO report.

Issues Reflected In The GAO Report

First, I would like to say that we believe the GAO did a thorough and professional job in researching and writing this report, and we value and appreciate their effort. We agree that the issues raised in the report are legitimate and valid issues that we must address. As is acknowledged in the report itself, we ourselves first identified some of those very issues and have been working to resolve them.

Revised Design Basis Threat Development Period

The first GAO report issue that I will address involves the period of time it took – almost two years – to develop and issue the new Design Basis Threat. GAO attributes this development period to delays in the intelligence community's efforts to develop an updated Postulated Threat, to DOE's application of its rather lengthy policy development review and comment process to the revision of the Design Basis Threat, and to sharp debate within DOE and other agencies regarding the size and capabilities of future terrorist threats and the availability of resources to counter those threats.

The Department's Design Basis Threat Policy is predicated on an interagency document titled *The Postulated Threat To U.S. Nuclear Weapons Facilities and Other Selected Strategic Facilities* (the Postulated Threat), developed jointly by DOE and other agencies, including intelligence agencies, and published by the Defense Intelligence Agency. Previous versions of the Postulated Threat were published as (interagency) policy, and consequently provided a substantial basis for our own Design Basis Threat policy.

Even before the terrorist attacks of September 11, 2001, there was considerable discussion within DOE of the need to update our Design Basis Threat. However, a thorough revision of the Design Basis Threat policy was dependent on the updating of its source policy, the Postulated Threat. In August 2001, shortly before the September 11th attacks, DOE initiated discussions with other agencies aimed at reviewing and revising the 1998 Postulated Threat. After September 2001, it was clear that the true nature of the terrorist threat was significantly different from that reflected in previous threat assessments, and the need to revise the Design Basis Threat to better reflect newly-recognized realities was beyond debate. There was a concurrent recognition among the agencies responsible for the Postulated Threat that it also needed revision, for the same reasons. However, the very events that highlighted the need to revise our threat policies – the terrorist attacks of September 11th – also resulted in the reallocation of the resources needed to revise the Postulated Threat to support real-time assessments of terrorist threats for national and international events. Consequently, efforts to revise the Postulated Threat were delayed for several months.

In January 2002 the Defense Intelligence Agency, assisted by DOE and other agencies, including intelligence agencies, resumed the effort to update the Postulated Threat. This effort took approximately one year and involved several revisions. During that period, DOE developed and internally circulated several drafts of a revised Design Basis Threat, each based on the (then) current version of the developing Postulated Threat. Each of these drafts was circulated among our appropriate program offices for review and comment. The Defense Intelligence Agency published the new Postulated Threat document in January 2003 as a report (a threat assessment) rather than as a policy as had been previous practice. DOE used the final version of the Postulated Threat to develop the final version of its revised Design Basis Threat, which was issued several months later in May 2003.

Even given the various circumstances and the complicated nature of this development process, and the necessity of knowing the ultimate parameters of the revised Postulated Threat before finalizing our revised Design Basis Threat, we acknowledge that this process took longer than we would have liked. The Secretary realized at the time that, even though this was a complicated development process with significant impact on future programs, operations, and budgets, progress was slow, and he monitored progress of the development effort through status briefings and updates. His concern about the pace of progress and the need to improve internal coordination of such matters was one of his motivations for creating the Office of Security and Safety Performance Assurance. It is important to note, however, that DOE did not wait for the publication of a revised Design Basis Threat to take action to increase security at our facilities. As described in the GAO report, on September 11, 2001, we recognized the changed nature of the threat and instituted a number of measures to increase physical security levels at our sites; many of those measures remain in effect. Some of those measures are manpower intensive and intended to be temporary in nature. Our deliberative process for implementing the requirements of the revised Design Basis Threat, now underway, will result in longer-term, more permanent, more sustainable, more robust, and more efficient and cost-effective upgrades to our protection systems.

Variances Between Threat Parameters in the Postulated Threat and the Design Basis Threat

The GAO report points out that although the magnitude of the terrorist threat described in the revised Design Basis Threat is greater than that described in the previous policy, it is smaller than that described in the current Postulated Threat. It also offers the opinion that the criteria DOE has selected for determining when a facility may need to protect against radiological, chemical, or biological sabotage may not be sufficient.

The differences in the parameters (e.g., numbers of terrorists, etc.) that appear in our Design Basis Threat versus those in the Postulated Threat result from the differing scopes and purposes of the two documents.

The interagency Postulated Threat is intended to serve as a reference for long-term planning and programming by U.S. security forces. It takes into account potential threats against U.S. assets worldwide, both inside and outside the U.S., and characterizes what that threat is expected to look like over a ten-year period. Given that scope, it assesses adversary capabilities in geographical areas where adversary groups are home-based, operate in locations where they receive a level of support from governments and societies, or operate in locations where there is little or no government control. In such environments, potential adversaries have expanded capabilities. Hence, the Postulated Threat identifies a range of adversary capabilities that is based on what is possible anywhere in the world.

The DOE Design Basis Threat has a different purpose. It is the design basis for DOE protection systems and a performance standard for established protection systems. As such, it defines specific adversary group sizes, equipment, and capabilities that must be countered with a high probability of success. Through extensive analysis using the best data available from the U.S. intelligence community, DOE analysts have established the current Design Basis Threat at a level that encompasses past terrorist events worldwide, requires sites located in the United States to design and analyze protection systems against specified adversary capabilities, and establishes a very high performance standard against that threat. In addition, the Design Basis Threat provides the protection strategy that must be used for each of several target types: examples of such strategies range from denial of access to establishing appropriate administrative controls. While the revised DOE Design Basis Threat takes into account a variety of sources and assessments, including the 2003 Postulated Threat, it is crafted to meet the Department's specific needs in relation to carrying out its protection responsibilities.

Regarding GAO's assertion that the criteria we are using to determine when facilities may need to be protected against radiological, chemical, or biological sabotage may not be sufficient, we can assure you that our intent is to employ appropriate criteria based on sound science. At present, much of that science is oriented toward establishing safe levels of release during normal operations and under accident

conditions. While the currently established criteria may not be the best for assessing malevolent acts, they do represent the current level of knowledge. For this reason, they were incorporated into the current Design Basis Threat while additional studies are conducted throughout the scientific community to determine whether they provide an appropriate level of protection against the actual threats depicted in the Postulated Threat and other intelligence community assessments. The Department is continually working with other government agencies to evaluate the criteria used for radiological, chemical, and biological sabotage determinations. In particular, the Department continually monitors government policy and legislation pertinent to toxicological sabotage and is committed to modifying our threat policy upon the issuance of new or revised standards. For example, we have developed a policy, currently in the final stages of comment and review, addressing the safeguarding of select biological agents and toxins. It is based on 42 CFR 73 and incorporates the best security practices of both DOE and the Centers for Disease Control.

We believe that the rationale used for the development of our current Design Basis Threat, described above, is sound and was the appropriate approach. However, we are continually looking for better ways to do things, and I have directed a review of this process to determine if this is still the best approach and if there is more we should be doing in this area.

Consequences and Effectiveness of Heightened Security Measures

While the GAO report credited DOE with taking immediate steps to improve physical security in the aftermath of the September 11th attacks, it indicated that those largely manpower intensive measures are expensive and have resulted in elevated levels of fatigue, retention problems, and reduced training for our protective forces. The report also indicated that the effectiveness of the increased Security Condition levels employed has not been assessed using formal vulnerability assessment tools such as computer modeling and force-on-force exercises.

DOE has recognized from the outset the large burden that was placed on our protective forces to implement the increased Security Condition levels in effect since the September 11th attacks. However, the situation required our line managers to act quickly to provide adequate protection for our facilities against the heightened threat, and that often meant employing measures that were designed for temporary use. The protection element that could be modified most quickly was the number of protective force members on duty. Therefore, unavoidably, some sites adopted measures that were costly, manpower intensive, and, over time, impacted the readiness levels of our protective forces. As the increased threat level continued, some sites took the initiative to modify other aspects of their protection systems to reduce some of the burden on the protective force. Additionally, the long process of hiring, clearing, and training new protective force personnel is providing some relief to the burden on our protective force personnel.

Acknowledging that the increased level of danger of a terrorist attack is not going to subside soon but will likely be with us for the foreseeable future, on September 8, 2003 the Secretary directed line managers and security professionals to emphasize finding or devising effective methods to make safeguards and security dollars go farther and to reduce the reliance on protective force manpower. He also directed my office to look hard at technologies that could be deployed to provide relief to the manpower burden issue and improve protection systems in other ways. I will discuss our efforts in that area in more detail later in my testimony.

The GAO was correct in asserting that when we implemented increased Security Condition levels, we had not formally analyzed or tested the effectiveness of those increased levels. However, our protection posture at higher Security Condition levels is more restrictive and more robust than our normal protection posture. Intuitively, therefore, we conclude that our protection posture at higher Security Condition levels will provide increased protection, but, in the press of time following September 11th, we did not apply our formal vulnerability assessment process to assessing the precise increase in protection before employing

them. Our formal vulnerability assessment process provides a comprehensive assessment of the protection system and is therefore very time consuming and expensive. Under normal conditions, DOE sites are required to employ it to ensure that their basic protection posture provides an acceptable level of assurance that it can defeat the applicable threat. As an essential element of Design Basis Threat implementation, DOE sites are now engaged in employing the rigorous vulnerability assessment methodology to evaluate every aspect of their protection systems, including the additional measures required to implement enhanced Security Conditions.

This additional vulnerability assessment effort requires more resources, and we recognize that one of our current weaknesses is a shortage of personnel formally trained to apply the very complex vulnerability assessment methodology. To address this need, I have directed our National Training Center (formerly the Nonproliferation and National Security Institute) to increase the output of security professionals trained in the application of this methodology.

Overarching Issues In Need Of Resolution

Finally, the GAO report noted that in order to meet the requirements of the new Design Basis Threat DOE needs to address several overarching issues, such as providing additional Design Basis Threat implementation guidance, creating implementation plans, and developing budgets to support those plans. The GAO report also expressed doubt that DOE's goal of meeting the requirements of the new Design Basis Threat by the end of FY2006 was realistic for some sites.

As the GAO acknowledged in its report, DOE had previously identified these specific issues and was already in the process of addressing them at the time GAO was collecting its data. In December 2003, formal training was provided to DOE vulnerability analysts in the improved vulnerability assessment process required to address the revised structure of the Design Basis Threat. In January 2004 the Deputy

Secretary issued additional guidance regarding the expectations and procedures for full implementation of the new Design Basis Threat. That guidance includes the requirement for each site to develop and maintain implementation plans that identify all tasks necessary to achieve full implementation of the Design Basis Threat and that establish realistic and measurable milestones necessary for the completion of all identified tasks. It further requires line managers, including Secretarial officers, to review and approve the implementation plans and to track the progress of implementation efforts. Progress toward achieving established milestones must be assessed, tracked, and reported on a quarterly basis, and quarterly reports must also include an assessment – based on the results of current vulnerability assessments, computer modeling, and performance testing – of the level of threat each facility is prepared to meet. Finally, the guidance requires our independent oversight organization to critically review site implementation plans, test the effectiveness of protection system changes that are implemented, and evaluate the ability of protection systems to protect against the level of threat claimed in the quarterly reports.

Sites have developed and submitted initial implementation plans, and these plans have been reviewed by the appropriate line managers, Secretarial officers, and by my office. In some cases, revisions to the initial plans were necessary to fully establish the analytical basis for the proposed actions and to supply additional detail regarding implementation schedules. These implementation plans are living documents. The initial plans reflect the best knowledge available at the time they were developed, and many were primarily based on existing vulnerability assessments updated by tabletop exercises, expert opinion, and performance testing. The results of ongoing vulnerability assessment activities, mission changes, consolidation of materials, or other factors may require modification of some aspects of some plans during the implementation period. Any necessary modifications to the implementation plans will be documented, approved, and incorporated into the plans through the quarterly reporting process.

Line management's review of the implementation plans and supporting documentation evaluated the projected costs associated with implementing the requirements of the Design Basis Threat. The plans include the justifications for needed upgrades and identify the most cost-effective upgrades necessary to achieve a high level of protection system effectiveness. The Department's FY2005 Congressional budget submission includes costs for planned security enhancements, and funds needed to complete full implementation of the Design Basis Threat, based on the results of vulnerability assessments now in progress, will be addressed in the FY2006 budget submission.

Regarding the ability of all sites to fully implement the Design Basis Threat by the end of FY2006, I must emphasize that we have established that as our goal and we have every intention of meeting it. The Department has made a very aggressive commitment in this case: we have identified what needs to be done, we have instituted a process to monitor progress toward individual milestones and toward the ultimate goal of full implementation, and DOE is committed to achieving all protection goals by the end of FY2006. If and when progress or the likelihood of progress falls below expectations, senior managers will take appropriate action. This approach has already led the Secretary to direct that special nuclear material be expeditiously moved from TA-18 at Los Alamos National Laboratory to the Nevada Test Site. If, as the end of FY2006 approaches, we assess that some facilities cannot fully and reliably perform to the requirements of the Design Basis Threat, the Department's managers will take immediate and appropriate action to mitigate urgent risks. These actions could include a wide range of management responses, including curtailment or modification of special nuclear material handling and operations, modifications to the protective posture, or any other compensatory actions necessary to protect our assets in accordance with the requirements of the Design Basis Threat.

SSA's Role in Design Basis Threat Implementation

While primary responsibility for implementing the requirements of the Design Basis Threat rests with our individual sites and their line management chains, the Office of Security and Safety Performance Assurance is responsible for assisting in this effort, monitoring progress, and validating the effectiveness of program enhancements. We have developed a three-phased approach to discharge this responsibility.

In Phase One, our Office of Security carefully reviewed the initial site implementation plans to determine if they fully met the requirements laid out by the Deputy Secretary in his January 2004 Memorandum. Whenever an implementation plan fell short of expectations in any way, the deficiencies were fully identified to the responsible program office so the plan could be appropriately amended. Phase One has been completed for the submitted plans.

During Phase Two, Office of Security subject matter experts review the supporting documentation accompanying each implementation plan. This activity typically includes analysis of vulnerability assessments to determine their accuracy, applicability, and appropriateness, and may include site visits as needed. If these reviews indicate the need for any modifications to the implementation plan, the Office of Security will work with the site to identify the specific modifications needed. Phase Two is well underway.

Phase Three involves ongoing technical assistance and validation efforts. The Office of Security will deploy multi-disciplinary safeguards and security teams – consisting of experts in physical security, protective forces, alarm command and control systems, and material management and control – to provide guidance and assistance on specific technical matters unique to each site. These teams will assist the sites and program offices in identifying appropriate ways to meet the long-term operational requirements of the Design Basis Threat. As I will discuss in more detail shortly, the Office of Security will also assist sites

in this effort by identifying and deploying existing technologies and developing and deploying new technologies that can increase the effectiveness and efficiency of protection systems. Additionally, the Office of Independent Oversight and Performance Assurance, through its program of scheduled oversight activities, will review progress toward achieving implementation plan milestones and will evaluate the effectiveness of protection program enhancements that have been implemented.

Key Efforts To Improve Security Performance in the Department.

In my testimony to this point I have addressed your specific interests in the issues raised and discussed in the GAO report. Those issues deal largely with events of the past. In my opinion, what the Department is currently doing to improve security programs and to facilitate the full implementation of the requirements of the revised Design Basis Threat are of more importance and relevance, and may be of greater interest to the members of the subcommittee.

The Department's senior leadership, including the Secretary, the Deputy Secretary, and the NNSA Administrator, is fully committed to properly discharging the Department's security responsibilities, including the timely and thorough implementation of changes necessary to meet the requirements of the revised Design Basis Threat. They have demonstrated this commitment repeatedly, over time, through a number of security-related initiatives. That commitment is reflected in Secretary Abraham's recent creation of my organization. While the Secretary properly holds line managers accountable for effectively implementing security programs, he recognized that the Department's efforts to improve protection programs could be accelerated and could yield more effective results if relationships and interactions between Headquarters elements and the field were improved. Secretary Abraham created my office – the Office of Security and Safety Performance Assurance – to implement his firm belief that Headquarters security resources, working closely and collegially with the field, could increase the timeliness and effectiveness of protection program upgrades and could ensure that appropriate security

technologies could be deployed where and when needed. His directions to me when he created the office resulted in four major new priorities for my office: to improve communications and cooperation between my organization and the field; to improve the quality of security policy and policy guidance; to evaluate and develop security-related technologies and make them available to the field in a timely manner; and to overhaul security training to ensure that national-level training resources are responsive to the needs of field organizations. We believe that improvements in these four areas are key not only to our current efforts to improve security and fully implement the requirements of the revised Design Basis Threat, but also to the future overall vitality and robustness of our protection programs. The importance of our initiatives in these areas and their pertinence to the interests of the members of the Subcommittee merit further discussion here, so I will more fully describe each.

Improved Communication Between Headquarters and The Field

First, we are improving the quantity and quality of (security-related) communication between my office (including my subordinate policy and independent oversight offices), other Headquarters staff and program offices, and field elements, including both line managers and security professionals in both Federal and contractor field organizations. It is critically important to our efforts to improve the effectiveness and efficiency of our protection programs that everyone in the Department with security program responsibilities fully understand each other's concerns and points of view, fully understand what is expected of them, and fully and openly share ideas, information, and lessons-learned to the benefit of the entire DOE community. The task of improving communications among individuals and organization is both easy and difficult. It is easy because the information that needs to be exchanged already exists, and simply has to be exchanged between the appropriate parties. It is difficult because the exchange of that information in some cases requires modifications of established patterns of interpersonal relationships, management-imposed information flow processes, and organizational relationships. We are working hard to ensure that all organizational relationships are mutually beneficial and supportive of

protection program needs. While numerous formal and informal communications mechanisms already exist, our goal is to make these more effective.

Improved Security Policy and Guidance

Our security policies and the accompanying implementation guidance are the foundations upon which our protection programs are built. We believe that our security policies across the board should be practical, based on real needs, implementable, and sufficiently clearly stated as to not be open to widely divergent interpretations. Some of our current policies fall short of this mark, and have been contributing sources to some of the delays we have experienced in improving our programs in some areas. A major contributing factor to the issues concerning policy was a past decision to prohibit policy developers from communicating directly with field sites. This speaks directly to the previously discussed focus area – improved communications. The Deputy Secretary recently directed a change to this ill-conceived practice, and we have established necessary dialogues to facilitate policy revisions and development. Our policy organization is already at work reformulating many of our security policies to make the needed improvements. Their instructions, as indicated above, are to ensure that policies are based on needs, practical, implementable, and clearly stated.

Introduction of Security-Related Technologies

The Secretary sees our ability to implement new security technologies as crucial to our ability to fully implement the requirements of the revised Design Basis Threat. We are convinced that improved technologies will be a long-term key in our efforts to improve the effectiveness, and particularly the efficiency of our protection programs. We have to move away – whenever possible – from manpower intensive responses to security concerns or elevated risks – the tendency to "add more guards." Manpower intensive responses are very costly and often not extremely effective. Permanent use of

additional manpower involves long lead times to hire and clear personnel, and short-term use of additional manpower often involves oppressive levels of overtime, which degrades individual performance. The introduction of new technologies such as active and passive barrier systems and others, can act as force multipliers that reduce our dependence on increased manpower levels. My office is charged with evaluating or developing such security-related technologies, making them available to the field for implementation in a timely manner, and assisting the field as necessary in their implementation. The Department has the scientific and technical resources to address our technology needs, and in fact we do development work in this area for ourselves and for other agencies. The NNSA Administrator, Linton Brooks, and I intend to improve our internal efforts in this area and provide the field with technological options that they can use to reduce manpower and improve the effectiveness of their protection systems.

This effort is already underway. For example, a current project at Oak Ridge illustrates our efforts in this area and the potential for more effective employment of technology. My staff is cooperating with project staff at Oak Ridge to incorporate more and newer technology into the design of the protection system for a building where special nuclear material processing will be conducted to allow removal of the material and eventual decontamination and decommissioning of the building. Clearly, a substantial cost savings can be realized for this project if other methods can be substituted for the expensive protection measures normally applied to a permanent facility. We are confident that, working together, my office and the line managers responsible for these operations will be able to devise a solution that will provide cost-effective protection while significantly reducing protective force manpower requirements. Other complex-wide efforts, such as our drive to consolidate special nuclear materials, will also help to reduce the protection challenge and manpower requirements.

Improved Security Training

The final focus area for major overhaul is security training. My policy organization, through its National Training Center (formerly Nonproliferation and National Security Institute), is responsible for establishing security training standards and for providing safeguards and security related professional training of various types. We intend to increase the efficiency and effectiveness of those efforts by ensuring that the way training resources are employed is more responsive to the specific needs of field organizations. To that end, I have recently appointed a well-qualified manager in my organization as Director of the National Training Center, and I have given him specific guidance regarding my expectations for the employment of these substantial training resources. Even prior to that appointment, we were moving to respond to needs in this area. As I mentioned previously, late last year we conducted specific training in new vulnerability assessment methodologies, and a related priority is to respond to the needs of the field by training additional security professionals in that very complex process.

We are focusing considerable effort on these four areas, and I strongly believe that the Secretary's instincts will prove to be correct and that these initiatives will have a profound effect on our efforts to strengthen our protection programs. We are already at work improving our performance in these areas. Most of the necessary infrastructure was already in place, and in some cases we just need to change some of our practices and ways of doing business to achieve our desired goals.

Concluding Remarks

As I conclude my remarks, I want to emphasize my belief in the sincere intentions and unprecedented efforts of the Department's senior managers to improve our protection program performance. The Department's leadership understands and acknowledges that the goal we have set for ourselves – to fully implement the requirements of the revised Design Basis Threat Department-wide by the end of FY2006 –

is a lofty goal. It is a challenging goal. To meet it will require both continuing management attention and support and a significant effort by many people throughout the Department. The Department's leadership has declared its willingness and determination to take the steps necessary to meet this goal, and has backed its declaration with action. The Secretary's issuance of the revised Design Basis Threat and the Deputy Secretary's direction to the Under Secretaries to respond to it immediately (e.g., to apply it immediately to new facilities and operations, to the restart of dormant facilities and operations, and to all vulnerability assessments occurring after May 2003) reflects a commitment and a resolve to make positive changes to the Department's security programs. The Deputy Secretary's stringent guidance on the process for implementing the Design Basis Threat for facilities and operations that could not implement it immediately, and the Secretary's creation of my office to expedite security-related improvements are further confirmation of an unyielding intent to improve the Departments protection program performance.

We have made significant progress toward implementing the revised Design Basis Threat at many sites, we are currently on track, and managers have demonstrated their willingness to make hard decisions to support the effort. Without minimizing the magnitude of the task ahead, we believe that the Department is approaching the task with confidence and a determination to succeed. We fully intend to pursue our efforts to improve our protection programs until we achieve a Department-wide level of performance that meets our own expectations as well as the expectations of Congress and the American people. Thank you. This concludes my prepared testimony.

Mr. SHAYS. Would you do me the favor, Mr. Podonsky, of describing what you are versus what Mr. Brooks is.

Mr. PODONSKY. I pause—you mean my function? For the Department of Energy, I report to the Secretary of Energy.

I have two offices. One office is the Independent Oversight and Performance Assurance Office headed up by Director Michael Kilpatrick, who is responsible for independently assessing the performance of the Department of Energy in environment, safety, health, safeguard security, cybersecurity, and emergency management.

Independence means that it's——

Mr. SHAYS. And environment as well?

Mr. PODONSKY. Environment as well. It's independent of the program offices. Their independence comes from how the work is conducted. They are not implementers of any of the policies that are promulgated by the Department.

My other office, the Office of Security, headed up by the Director of Security, Marshall Combs, is responsible for promulgating policy as well as providing technical assistance to help the field in its implementation of DBT and other policies.

Ambassador Brooks is an implementer. He is many things, but in that regard he's an implementer. We are the policy promulgators and the overseers.

Mr. SHAYS. Wait. He is not policy?

Mr. PODONSKY. According to the NNSA act, he generates policy for his agency, but the Department policy, being from a Cabinet official and according to the act as I understand it, the Secretary has overall policy of the Department, which would include NNSA.

Mr. SHAYS. Ambassador, in your words, how do you define yourself versus Mr. Podonsky?

Mr. BROOKS. He helps the Secretary set policy. I implement. He comes and checks to make sure I've done it right.

Mr. SHAYS. Would the design basis threat—you both—tell me your roles in establishing the design basis threat.

Mr. PODONSKY. I've been in this job for 4 months. So my job previously I was a critic of the design basis threat as the overseer.

Mr. SHAYS. That's one reason why I was getting confused here.

Mr. PODONSKY. I'm schizophrenic, too, sir.

Mr. SHAYS. I didn't say that.

Mr. PODONSKY. The Office of Security promulgated the design basis threat for the Department in coordination with other agencies and then coordinated, as you've heard in testimony by GAO, with the other elements of the Department.

Mr. SHAYS. Who initiates the design? Do you initiate the design basis threat?

Mr. PODONSKY. My Office of Security initiates the design basis threat.

Mr. SHAYS. So it's not Ambassador Brooks that does that?

Mr. PODONSKY. No.

Mr. SHAYS. What roll does he have, in your words, with design basis threat?

Mr. PODONSKY. I believe Ambassador Brooks as well as the Under Secretary for ESE has the responsibility to implement the Secretary's policy, and the design basis threat is the Secretary's

policy on what the posture of protection should be in the Department.

Mr. SHAYS. The design basis threat basically determines what the threat is. Do you also determine what the antidote to that threat is or is that Ambassador Brooks that does that?

Mr. PODONSKY. I need to clarify. The design basis threat is quite a misnomer, the word "threat." Design basis threat is really a DOE performance standard. The threat is developed by the postulated threat document that is created by the Defense Intelligence Agency. So what the Department is—they take the postulated threat, and they evaluate what's contained in the postulated threat, and they specifically are applying it to the DOE sites and the protection of those sites.

Mr. SHAYS. That's a little different than I basically had always viewed it, and so I'm just exposing my ignorance, which happens quite often. But I do want to understand it.

My view was the design basis threat was we would say that it was likely that at, say, Y–12 you might have up to so many people, you might have so many people in-house, out of it, and we would give the worst-case scenario, and then you would have to design a way to prevent that threat from succeeding. Now you're telling me that the postulate—that you don't determine that at all. That's someone else outside your organization that does that?

Mr. PODONSKY. No, sir. Let me clarify, and I think in the last panel there was also a question as well as the GAO question why the numbers in the postulated threat differ from the DOE design basis threat. And it might be helpful if I described the postulated threat as the document that characterizes what the threat is expected to look like, and it's intended to portray a range of adversary capabilities.

Mr. SHAYS. And you would agree that's a key assumption?

Mr. PODONSKY. Yes, sir.

Mr. SHAYS. Because you could design a threat to just be almost meaningless and easy to come back or you could have a threat that would be almost beyond absurd that you could never defend against.

Mr. PODONSKY. And I think that's probably part and parcel why it took such a long time for the Department of Energy to publish its design basis threat, and there's some other factors that I could go into later.

Mr. SHAYS. I don't think it should take so long sir. I mean, that's one thing I could never accept, not in this day and age with the threat existing. But, anyway——

Mr. PODONSKY. But getting back to your original question, sir, if I might, the design basis threat for the Department gives the specific adversary group's size, equipment and capability; and then the DOE analyst established that design basis threat at a level that considers all the terrorist events worldwide. And then they apply it to the different sites with specific——

Mr. SHAYS. Wouldn't it be logical, though, without talking numbers, that terrorists are going to—they did what they needed to do to accomplish their mission? For instance, you only need two people on the boat evidently with a bomb to go up to the Cole. You don't need 1,000. That doesn't mean they won't use 1,000 but they didn't

need to use 1,000 to do that. Or you only needed five people per plane—in one case only four—but five people per plane and you could take a plane. So they determined what they needed to overcome any—to accomplish their mission.

Wouldn't it be logical that terrorists would look at a facility and say, well, my gosh, we may need 50 people in order to succeed here; and am I to interpret because they never used 50 somewhere else that we make an assumption that they won't?

Mr. PODONSKY. No, sir. I think what has to happen is you have a point in time that you can put so much security in place that you end up not being able to do your mission. And somewhere the decision has to be made, is what is the Department—what agencies—what risks are you willing to accept, and there has to be a tradeoff.

I'm not here to defend the current DBT as much as I would also like to say that the DBT, the current DBT, was published in May 2003, is now almost reaching a year. And I would tell you that when the authors of the original DBT put it forward to the Secretary, the Secretary of Energy actually increased numbers, without getting into specifics, which was quite a surprise to the safeguard security community that he actually increased it.

I've also been told as of this morning that I would like to share with you that, as a result of your work and the GAO's report, I am directed in my new capacity to take 30 to 60 days to reexamine where we are with the DBT and to see whether or not the numbers need to change now that we've had a year of experience and what does it mean.

Mr. SHAYS. Again, I'm getting a little confused, because the issue of the size and equipment and capabilities is not determined by you; correct?

Mr. PODONSKY. It's determined by the intelligence community.

Mr. SHAYS. Right. So the intelligence community—I think somehow having the intelligence community determine this makes me less comfortable, and I don't mean to be cute. You are then supposed to find the antidote to that; correct?

Mr. PODONSKY. My staff, yes, sir.

Mr. SHAYS. That's your staff, not Ambassador Brooks.

Mr. PODONSKY. Yes, sir.

Mr. SHAYS. So now what is ironic is you're being asked to look at the design basis threat and not the intelligence, and that's why I'm getting confused. If it's their job, why are you being asked——

Mr. PODONSKY. I think because of the commitment of this administration to security and the reality of the word today, they recognize that we need to reexamine where we are. As I said in my opening statement, we agree with the points made in the GAO report.

Mr. SHAYS. I would think when setting design basis threat, you would look at your capabilities and then you would say, my gosh, how could someone beat our capabilities? That's the way I would think that a terrorist would do. They would want to get information about how you secure a facility and then they want to say, OK, what do we do to beat your preventative measures? Then, what I would think they would do is they would say, well, we would have to do these things. Then they would have to determine whether it is feasible or not, and you would have to determine the same thing.

You would have to be trying to anticipate what the terrorists would be doing.

For instance, in a site where there is not much of a buffer, and where you can get to the perimeter very easily, I would think the terrorists would say, well, it would take—I'm just going to just take something that that has no intelligence behind it—it's going to take 50 people. They're then going to go and say, well, can we then logically amass 50 people? And you're going to do the same thing, and you're going to know at what point they have no capability. I would think that's ultimately how you would determine the threat.

But what I'm hearing you say is that we're seeing what they have done in the past; and if they didn't, for instance, amass 50 people, then we may make an assumption they are not going to use 50 people, which strikes me as a hope and a prayer.

Mr. PODONSKY. No, sir. That's not what I'm implying. If that's what you're interpreting from my statement, then—then let me try to clarify that.

Historically, as we all know, on September 11 we were all surprised and shocked at what transpired. When we talk about the design basis threat, it's more than just adding numbers. It's exactly what you're saying. There's a lot of analysis that goes into targeted attractiveness, the potential paths that would take place; and if I might, if you'll allow me, I will give you one vignette.

In 1996, wearing my oversight hat, we went out to test the performance at one of our sites; and we brought with us the Navy SEALs. And the Commander of the Navy SEALs—we were testing against the previous design basis threat; and the Commander of the Navy SEALs said, Mr. Podonsky, if I was going to take this facility, I would bring in whatever number I needed to take the facility, which supports your statement. But we still have to balance what is the likelihood of an event and what's the amount of people that they are likely to amass and what do we want to protect against and there is a degree that has to come; and while I do not know anything to prove that there was money driving the numbers for design basis threat, it would be inconceivable to me that money could not be a consideration at some point.

Mr. SHAYS. Money has to be, ultimately. Otherwise, we could do an absurdity and say we'll have 10,000 people guard each site. Well, obviously, they would get in each other's way and probably be a danger, but money is a factor, and if we don't admit that, we're not being honest.

Ambassador Brooks, help me out in this conversation. When I traveled with you and we talked about design basis threat, I felt that you had a say in the design basis threat. And, by the way, help me out in this postulated threat or design basis threat. Walk me through that.

Mr. BROOKS. Certainly, sir.

First, let me talk about the internal organization of the Department. You have to distinguish between formal responsibility and where the Secretary turns for advice.

The formal responsibility for preparing the design basis threat document was with the Office of Security at the time, prior to Mr. Podonsky's arrival, a separate stand-alone office reporting to the Secretary. The Secretary, however, as is his practice, turns to his

senior subordinates for advice. So when the Office of Security prepared the draft of the design basis threat, the Secretary asked for the views of the then Under Secretary Card, he asked for my views and, he asked for the views of the Deputy Secretary. So I did have an opportunity, as I do on most policy things, to make my views known, even though I might not be formally responsible for developing that particular policy; and that's fairly common within government.

Further, since I am responsible for making sure that we are implementing the Secretary's policy, I need to understand it well and so, when we traveled, I attempted to articulate it to you.

Now let's talk about postulated threat and design basis threat.

A group from the intelligence community—and Mr. Podonsky and I have met with the analysts who actually did this and walked through exactly what they did to make sure that we understood at a classified level where there was data and adversaries where there was judgment. We were advised of their views on what might do and might not do. And we were told that in some places there's just no data, you're not on your own, and there's a little of all of that in the postulated threat.

A group of analysts from the intelligence community with community support looked at what is the plausible threat worldwide over the next 10 years—and those two words are very important: the design basis threat—then looked and said, what is the problem we have to deal within the United States? For example, they said one wouldn't expect to see no cooperation from the government for terrorists, as might be true overseas; no meaningful support for terrorists within the population, as might be true overseas; no nearby logistics facilities, as might be true overseas.

So, after analyzing it, the Office of Security came to some conclusions about what would be an appropriate threat that the Secretary should promulgate to govern security at our sites. The Secretary, who is not a captive of his staff, took that, talked to a bunch of people, listened to a bunch of people and made, as Mr. Podonsky said, some judgments; and then that became his policy, and our task is to implement it.

So the postulated threat was the basis from which the design basis threat evolved, but the design basis threat is the Secretary's formal guidance to us about how to allocate resources.

Mr. SHAYS. As you both are responding to these questions, I think I'm having a sense of why I feel uneasy; and so maybe you can respond. It strikes me that the postulated threat is based on what we have seen terrorists do. If we followed that logic, it would explain why we would never have been prepared for September 11. Because we basically said, terrorists as a general rule, don't know how to fly planes, and as a general rule we haven't seen five of them take a plane and use it as a missile. But, in fact, they did that. So if the postulated threat is based on historic practice—I would be very uneasy.

Mr. BROOKS. Yes, sir. I want to choose my words very carefully, remembering this is an open session; and we may want to go into this more later. The word postulated is important, and it is not limited to what has been seen in the past.

Mr. SHAYS. Fair enough.

Mr. BROOKS. It uses what has been seen in the past to inform, to make some postulations about what might happen in the future and provide some nonquantitative estimates of probability. But I think if the analysts who were working it were here they would want to distinguish between documents traditionally done by the Intel general community, which are based on, as much as possible, evidence and a document which says, based on the evidence, what is plausible and is therefore a postulated threat. The word in this particular case actually means something.

Mr. SHAYS. I'm going to get to your going through the response to GAO. But let me ask you, again, is it your job to defend these sites or is it Mr. Podonsky's job?

Mr. BROOKS. My job.

Mr. SHAYS. So, basically, the design basis threat ultimately goes through his office. It's your job ultimately to defend against the threat. And then, Mr. Podonsky, is it your job to see if they can do that?

Mr. PODONSKY. Yes, sir, to independently test Ambassador Brooks' facilities as well as the rest of the Department's facilities.

Mr. SHAYS. So now I'm getting a sense that the two of you disagree a little bit on the GAO's findings, is that fair?

Mr. BROOKS. I don't think that is true.

Mr. SHAYS. OK. I heard basically agreement with GAO from you, Mr. Podonsky, and I heard Ambassador Brooks' disagreement with GAO.

Mr. BROOKS. That may have been inelegant phrasing on my part, because I didn't hear Mr. Podonsky say anything I disagreed with.

Mr. SHAYS. OK. So tell me what you agree with within the report—and I'm looking at page 27 where it's first, second, and third. Would you go through each of those and tell me what you agree with; and, finally—there's four points—and the conclusions.

Mr. BROOKS. I have seven recommendations listed. I may not actually have the exact same version of the document you have.

Mr. SHAYS. Let's just go through it. So, "First, DOE needs to know the effectiveness of its most immediate response to September 11, 2001, the move to higher SECON levels. The higher SECON levels, while increasing the level of visible deterrence, have come at a significant cost in budget dollars and protective force readiness. We believe that DOE needs to follow its own policies and use its well-established vulnerability assessment methodology to evaluate the effectiveness of these additional security measures." Do you disagree with that?

Mr. BROOKS. I think that's a good recommendation, and we ought to do it.

But I also agree with the comment that you heard from the previous panel that in the near term, as a practical matter, the only way you can increase security protection in the short term in response to threats is more people, and that's essentially what we get with SECONs, but I think that we are spending a lot of time and energy on it and formally understanding how effective that is is a perfectly reasonable thing. I think—would you like me to just go down the——

Mr. SHAYS. Just go down. So the second——

Mr. BROOKS. I have no objection to looking at how the DBT was developed.

Mr. SHAYS. This is a second——

Mr. BROOKS. The second bullet that says, "Review how the DBT is developed to see if this policymaking approach is appropriate." I think that, whatever may or may not have been appropriate for a radical change that was represented by September 11, we're probably going to be looking at incremental changes. So I think that's a perfectly reasonable thing to do. I'm not sure it will make a huge deal of difference.

The most important recommendation and the one in which—and I'm speaking personally, because the Department hasn't taken a formal position on these. I believe that the graded threat approach is appropriately applied, for reasons I said in my statement, to improvised nuclear devices.

Mr. SHAYS. It says, "Reexamine the current application of the graded threat approach to sites that may have improvised nuclear device concerns." And you agree or disagree with that?

Mr. BROOKS. I have no objection to reexamining anything. I believe that when we reexamine it we will find that we were correct.

Mr. SHAYS. You're not going on like Allen Greenspan on me and talking in tongues, are you?

Mr. BROOKS. No, sir. I think we're right.

Mr. SHAYS. So the bottom line is you accept that they need to reexamine, but you don't think they need to?

Mr. BROOKS. You always ought to look at everything, because otherwise you fall into complacency. I do not share the underlying assumption of the GAO that we're applying this methodology imprecisely.

I'm going to defer to Mr. Podonsky on chemical and biological.

Mr. SHAYS. Here's what I'm going to do. Let me do this. We have one, two, three, four, five, six, seven recommendations. Do you agree with all of these recommendations; and, if not, which ones do you not agree with?

Mr. BROOKS. Yes, sir. I agree that we should examine the graded threat approach as it applies to improvised nuclear devices, because serious people have suggested we ought to look again. But from what I know so far, I remain convinced that we are correct.

The rest of the recommendations, I don't disagree with any of them, although I defer to Mr. Podonsky on the comment on biological and chemical.

Mr. SHAYS. Let me ask you, on all of the seven, where do you come down?

Mr. PODONSKY. Well, maybe this is from all of the years of my oversight, so we are partially the internal GAO, but I agree with all the recommendations that we need to be—that we need to look at these carefully.

Mr. SHAYS. Are you as confident as Ambassador Brooks is that reexamining the current application of the graded approach to sites that may have improvised nuclear device concerns, that's not—we're not going to find much?

Mr. PODONSKY. I don't share the same convictions that we may not find much. I'm a strong believer that we need to evaluate it in

the light of the year experience that we've had since we published the DBT.

Mr. BROOKS. I don't disagree with that.

Mr. SHAYS. So, basically, all of these recommendations you concur with but maybe not with the same level of enthusiasm.

When Ambassador Watson heard there was an ambassador Brooks, she decided to come down quickly. Why I am grateful is it enables me to have her presence here but also to note for the record a quorum is present and then be able to take care of some business before I recognize Ambassador Watson and—Congresswoman Watson.

I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record and the record remain open for that purpose. Without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted include their written statements in the record. Without objection, so ordered.

You have the floor. I thank you for coming.

Ms. WATSON. Thank you so much, Mr. Chairman.

I just wanted to underscore what the chairman said. I think it's essential that we reexamine all of our systems, methodology and so on in light of the newer warnings that have occurred in the last 48 hours that the target will be the United States. They're looking for soft spots.

I just returned from Vegas, a wedding, and I asked about the power outage, and the taxi driver said that wires were cut, and it was an inside job.

So we need to go back over—and I know that procedures were probably acceptable, but we cannot be too cautious, and I would encourage you—and I think you are all in agreement that the recommendations need to be reviewed, and I would encourage all different departments and units to just go back over and look at their security systems.

I thank you gentlemen very much. I'm sorry I wasn't here for the opening of the hearing, but I want to encourage you to support these recommendations sincerely.

Mr. SHAYS. I thank the gentlelady very much for, one, coming and making that point, and being here.

Ambassador, both my staff and I had a question on your opening statement; and I'm just going to have counsel just ask you a question. It was kind of curious.

Mr. HALLORAN. Thank you.

There's a sentence in the second paragraph of your submitted statement which you read. It says, "Today no nuclear weapons, Special Nuclear Material, or classified materials are at risk anywhere within the nuclear weapons complex." I think I understand what you're saying, but you're not saying there's no risk. Could you decode that for us?

Mr. BROOKS. I am not saying that there is no risk. There's always risk. What I am——

Mr. SHAYS. He's trying to be like Allen Greenspan.

Mr. BROOKS. Well, what I'm trying to convey is that there is no material that is not adequately protected, that the people who protect it are well trained and confident, that people looking, as Con-

gresswoman Watson said, for soft spots would be ill-advised to come to the sites for which I am responsible, because they aren't soft spots. But I am also trying not to pretend that there isn't work left to be done because there is. That's what I was trying to convey with that.

Mr. SHAYS. Because the bottom line is, the design basis threat, we're not going to even come close to reaching the requirements there for a few more years——

Mr. BROOKS. At all of the sites. A couple of them are close now.

Mr. SHAYS. And you have agreed with GAO that we need to reexamine the design basis threat?

Mr. BROOKS. That's correct.

Mr. SHAYS. So you're saying we need to reexamine it, and you acknowledge with GAO that we're not even going to reach that—living up to the existing design basis threat in the timeframe we had hoped to; correct?

Mr. BROOKS. I want to be very precise, Mr. Chairman—we are going to be prepared to meet our obligations under the Secretary's policy about the end of fiscal year 2006. We're going to, in some sites, do it sooner. We're going to put compensatory measures in where we can't meet it until 2006.

I do not share the skepticism that I discern in the GAO report that we're not going to meet the 2006 date. But that's 2006. This is 2004. So, obviously, we're going to make improvements over the next 2 years. I'm not suggesting and did not mean to imply that we have done everything yet.

Mr. SHAYS. Let me have Ms. Watson ask a question.

Ms. WATSON. Mr. Ambassador, in the light of the new threats, is there a possibility that we would review people who are responsible for the various security systems and do an in-depth review of who they are? You know, I just am very sensitive since I was told it was an inside job. So do you check those responsible and check them out, too, the new hires as well?

Mr. BROOKS. Yes, ma'am. We do that in three ways.

One is, of course, all the people in positions where they could influence this hold "Q" clearances, which involves a background investigation; and we update that periodically.

Second, those people who have direct access are in the Human Reliability Program, which provides a constant monitoring.

And then, third, as a matter really of nuclear weapons safety, in addition to security we use a concept where no single individual—call it the two-person rule—where no single individual can have an unimpeded access to a weapon in a way that would allow causing a detonation.

So we have a kind of a constant procedure to guard against the danger from insiders; and we do look at people, as you suggest.

Ms. WATSON. Thank you.

Let me just ask this: Is the 2006 goal based on the cost of reviewing the security? Why 2006?

Mr. BROOKS. Because that appeared to the Secretary to be when you could plausibly get there. I mean, there are some things that you can speed up by throwing money at them; and there are other things that you simply can't. If you want to improve physical systems, it takes time. If you want to look at protective forces and say

they need different equipment and need to be trained on it, it takes time. So 2006 was intended to recognize that we were trying to make a fairly significant improvement in security and that anything that can implement overnight isn't hugely significant, so the idea was to give us time to get there.

Ms. WATSON. I don't think 2 years is overnight. I just feel that in this era where we're being threatened, internationally and nationally, too, we might want to speed up.

I'm from California, and we have earthquakes all the time. The former Governor said, well, we're going to have phase one, phase two, phase three of resupporting the freeways. Well, wouldn't you know, there was an earthquake, and the freeway went down, and we were No. 3. It was an earthquake, and it went down in the center of my district. So I am saying everyone needs to have a No. 1 States, all of the various freeway sensitive spots.

So I'm thinking the same thing during this time when we have been threatened and we know these threats are very real. Maybe we want to speed that up. And you don't even need to respond. I just wanted to throw that out.

Thank you very much, Mr. Chairman.

Mr. SHAYS. Let me just tell you how we're going to conclude. The counsel is going to ask two more questions. I'm going to invite the other panel up if they want to make a comment before we go behind closed doors, because they may want to put something on the record that we can ask behind closed doors.

Mr. HALLORAN. Ambassador Brooks, in your initial list of things you wanted to comment on the first panel, you said that the nonbermfacility at Y–12 was still adequate. So I would ask if you could supply for the record a little more thorough explication of that in terms of what you're doing to respond to the IG's report and to rebut my simple assumption that underground is better than aboveground in terms of what's more secure.

Mr. BROOKS. Certainly. That's—I'd be happy to provide that for the record.

Mr. HALLORAN. Thank you.

And also a clarification of the——

Mr. BROOKS. Excuse me. May I make a point?

The assumption that underground is better than above ground is perfectly valid. Unfortunately, the difference between the two competing designs aren't limited to that, and that's the reason why I believe that the design we're now pursuing is superior, and we'll lay that out in some technical detail for you on the record, sir.

Mr. HALLORAN. Thank you.

[The information referred to follows:]

COMMITTEE: HOUSE COMMITTEE ON GOVERNMENT REFORM, SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

DATE: April 27, 2004

WITNESS: Linton F. Brooks
PAGE: 84, LINE: 1931

INSERT FOR THE RECORD

The current design for the Highly Enriched Uranium Materials Facility (HEUMF) at the Y-12 site is an above-ground design and some questions have been raised about the security effectiveness of this design. I would like to make several points.

The current design is based on the defense-in-depth security concept. Sandia National Laboratories has conducted extensive analysis to confirm that the current design will meet the current Design Basis Threat (DBT) requirements, and has more flexibility to respond to future DBT changes. The bermed design, on the other hand, would require a larger protective force to meet the current DBT requirements.

With the bermed design, as conceived, we would have difficulty incorporating upgrades to the facility's protection system in the future. Making the bermed concept respond well against a larger threat (beyond the current DBT) would likely require incorporating features similar to those for the current design or designing the facility as a secure underground facility.

If we upgraded the original bermed design, to include features similar to those in the current defense-in-depth design, the capital cost would be approximately $10 - $11 million more than the current design.

Since the bermed facility would require more guards, the life-cycle cost associated with the bermed design would be approximately $23 - $70 million (present value) more than the life-cycle cost associated with the current design.

Putting the HEUMF construction on hold while performing redesign and/or more detailed studies to further develop a detailed configuration and cost of a bermed facility could result in a project delay of up to 2 years. The additional cost associated with a 2-year delay and engineering cost for redesign is estimated to be $30 - $35 million.

The current design provides the lowest life cycle cost of the options considered to address the current DBT, and the design decision made in 2001 has been revalidated.

Assistant Secretary's initials: Preparation Lead: NA-55
Office Phone: 202-586-3476 Preparation Team: Tim McCune, NA-55
Concurrences: Bill Desmond, NA-55
Date Question Received:

Mr. HALLORAN. The other matter would be in terms of the schedule to remove all the material from the TA–18. There was a question in the first panel about whether it's just 50 percent and the intention is to keep 50 percent there past 2010 or whether the plan is to move it all.

Mr. BROOKS. The plan is to move it all. Where 50 percent comes from is we're going to remove 50 percent before we get the capability relocated to do what we're doing. That will reduce the number of storage facilities at TA–18 from two to one. That will take away from the diversion scenario, and so that will be a real improvement in security. Then we'll move the rest of it after we have reestablished the capability that's now at TA–18 to Nevada. That's where the 50 percent comes from. But we're going to move it all.

Mr. SHAYS. Let me ask, is there anything that either of you would like to put on the record in this open session before we meet later?

Mr. PODONSKY. Yes, Mr. Chairman. I would like to say one thing. It's an iteration of what I said earlier.

We recognize that under your leadership this committee is taking a very serious look at national security and security within the Department; and as a career member of DOE, not a political appointee, I want to emphasize the tremendous focus that this Secretary and the Deputy Secretary and Administrator Brooks have put on security. I think my colleagues from POGO as well as the GAO can testify to the fact that we have not seen this before. This is unprecedented within the Department's leadership.

Mr. SHAYS. Thank you very much.

I concur with your statement that there's a tremendous amount of hard work. I would just say to you in public that I believe that we have too many sites, and I believe our sites are so antiquated that they pose a risk. I realize, Ambassador Brooks, in the process of consolidating, that takes a tremendous amount of time, but I don't want you to wait until my daughter is 20 years older or if—I want you to at least get it done when she's 10 years older. I realize those are political decisions as well, but I would hope the Department would—the professionals would weigh in so at least there's a record so the politicians will have to respond to it.

I thank you very much, and I'm going to invite the other panel to come up just to see—and we'll see both of you a little later. Thank you.

Ambassador Brooks, I understand you may have to leave fairly quickly after. Are you going to be there in the beginning of that open session?

Mr. BROOKS. I was not intending to be there, Mr. Johnson will be there in my place.

Mr. SHAYS. That's fine. We understand the reason why, and that will be fine. Thank you for being here.

I want to make sure that there's not anything we should put on the record. Ms. Brian, I will start with you, since you're sitting down first.

Ms. BRIAN. Thank you very much, Mr. Chairman, for the opportunity.

I just wanted to submit for the record both the Inspector General's report on systematic cheating of the—by the security guards

at Y–12 as well as this April 9 memo by Dr. Everet Beckner regarding the relocation of materials at TA–18, that he's moving 50 percent over 18 months, and the Secretary of Energy, however—is that he wants all of it moved in 18 months.

[NOTE.—The Department of Energy report entitled, "Inspection Report, Protective Force Performance Test Improprieties," may be found in subcommittee files.]

Mr. SHAYS. When we talk about cheating, we do know that there has been some cheating. Is the word "systematic" used by——

Ms. BRIAN. They talk about repeated instances.

Mr. SHAYS. Repeated instances is the way we'll both define it then, OK?

Ms. BRIAN. That's fine.

And I just wanted to make two final responses that were made. One is with regard to the materials at Lawrence Livermore and the inability of the scientists to perform their work unless it is there. Those critical—what's considered by NNSA as critical experiments are also taking place at Los Alamos; and I'd also like to point out that if—the materials needed to also be done by Livermore scientists. If the material were moved to the Nevada test site, those few scientists that are actually working with those materials could take a 1-hour plane ride to Nevada to do that work.

And the second point I wanted to respond to was in the graded approach between a nuclear weapon versus nuclear materials, I just wanted to say that you don't need to make the materials into the configuration of a weapon to create an improvised nuclear device. You can do it within minutes.

Mr. SHAYS. Fair enough. I'm not sure Ambassador Brooks would disagree with that. If he would, he might want to come up.

Ms. Nazzaro.

Ms. NAZZARO. Yes, thank you, Mr. Chairman. I have two points I'd like to make.

First, we are very optimistic that—by the fact that DOE is now not only accepting but agreeing with our recommendations. I think that goes a long way to starting off on the right foot here.

The second is, regarding the discussion you had earlier on the postulated threat versus the design basis threat, we do want to make note that it is recognized that the postulated threat is a worldwide assessment, and it does apply to the United States, and in the past DOE has matched one for one, the postulated threat with the DBT. This is the first time that they had deviated from that.

Mr. SHAYS. And the significance of that is?

Ms. NAZZARO. Why is DOE making a determination now? When you have the intelligence community making this postulated threat, why is it that DOE thinks that they have more information or better information, that they don't need to guard against such a threat?

Mr. SHAYS. One more question—I guess we will get to that in the closed door, and that is very helpful for you to bring up, Mr. Noel.

Mr. NOEL. Just one other thing, we were talking about risk earlier. I mean, a point that we made in our report is that, basically by definition now, the Department facilities are at a higher level of risk because they are defending still at the old DBT. We now

have a new DBT at this level, and it is going to take them a couple of years to get there.

Mr. SHAYS. And that may not be high enough. Correct?

Mr. NOEL. Well, we are asking them to reexamine that in the two specific situations. And so to say that nothing is at risk is just not true.

Mr. SHAYS. It was; we are giving the Ambassador a little poetic license. I think I know what he was trying to say. And I don't usually put words in witnesses'—I think what he was trying to say is, don't think our sites are vulnerable and an easy target. But I do know that the Ambassador knows that we would clearly not be going to a new design basis threat, and we aren't there yet.

So, therefore, if we think even that design basis threat is a logical threat and we are not there yet, we are at risk of not being at that level. But, you know, he is also trying to make sure that people don't think that it's an easy target.

Mr. NOEL. No. And we would certainly—these are very heavily defended targets by very well-trained people.

Mr. SHAYS. Right. But we are, I believe, at risk. And until we get these sites exactly to the conditions we want, I think we are at risk.

Thank you all very much. We are adjourning this hearing, and we will convene a briefing, not a hearing, behind closed doors at 1:30.

[Whereupon, at 12:05 p.m., the subcommittee was recessed, to reconvene at 1:30 p.m., the same day.]

○